HOCHSCHULE für Angewandte Wissenschaften
Fachhochschule LANDSHUT · UNIVERSITY of Applied Sciences
Hochschule für Technik, Sozialwesen, Wirtschaft

FAKULTÄT Informatik

UNIVERSITY OF APPLIED SCIENCE LANDSHUT

FACULTY FOR COMPUTER SCIENCE

Can the Microsoft Azure Security Suite be a practical solution for SMBs when analysing and protecting existing IT infrastructure?

BACHELOR THESIS

submitted by Paul A. Eisenmann

submitted on the 31. of March 2022

University supervisor:
Prof. Dr.-Ing. J. Uhrmann

Industry supervisor:
IS4IT GmbH & N. Herpich, B.Sc.

"DYING AND SHUTDOWN IS ABSOLUTELY SAFE"

my utter most gratitude for your emotional support goes to:

FA, FS, JU, LH, NH, NN, SM & TE

Quote by Architects (modified)

BACHELOR THESIS DECLARATION

ERKLÄRUNG ZUR BACHELORARBEIT

(according to § 11, Abs. (4) 3 APO)

Student surname, first name: **Eisenmann, Paul Andreas** (* 13. Jul 1999)
Students number: **1114424**

Landshut University
Faculty of Computer Science

Hiermit erkläre ich, dass ich die Arbeit selbständig verfasst, noch nicht anderweitig für Prüfungszwecke vorgelegt, keine anderen als die angegebenen Quellen oder Hilfsmittel benützt sowie wörtliche und sinngemäße Zitate als solche gekennzeichnet habe.

I hereby declare that I have written this thesis independently, that I have not submitted it elsewhere for examination purposes, that I have not used any sources or aids other than those indicated and that I have marked literal and analogous citations as such.

....

(date) (student signature)

ABSTRACT

Small and medium sized businesses (SMB) face ever growing cyber security risks and are for this reason longing for solutions to mitigate those risks. Thus, it is this thesis' goal to investigate whether the cloud-based security tools offered by Microsoft Azure can fulfil the task from a technical point of view.

For this examination, two main research routes were chosen. The first route looks at security from a tool perspective and through practical case studies in SMB IT environments that include five common threats and needs of cyber security: hacking, phishing, viruses, monitoring, and internal threats. The second route investigates questions about full cloud-based security usage and implementation from a policy and compliance standpoint. It also offers practical solutions and considerations of SMB IT administrators and business leaders.

This thesis research result is that the Azure security suit offers a decent toolset for SMB IT security. However, the actual technical tool choice is only secondary in consideration, since the human component remains to be the one having to prevail against most cyber threats.

TABLE OF CONTENTS

1. INTRODUCTION

1.1 MOTIVATION

One trillion US Dollars. That's a one with twelfth zeros to it. More money that anyone can ever imagine. But it is the amount that was estimably lost by the world economy in the year 2019 due to cybercrime (McAfee, 2020). But the rising risk of cybercrime, threats related to incidents targeting IT infrastructure and dangers to information security are not only about financial threats to global companies. S&P500 companies invest a lot of money in their IT security infrastructure and are well equipped for ordinary cyber attacks (BKA, 2021). Even governments around the globe are responding to the emerging cyber threat with the establishment of agencies to protect critical IT infrastructure and helping the industry to respond to security incidents. Examples would be the CERT team of the BSI in Germany, the CISA in the United States of America and the NSCS in the United Kingdom (Diogenes & Thomas, 2021, p. 7).

Besides fraudulent attempts to steal money and information from companies, cyber security has become an essential part of global security policy in general. Maintaining a state funded 'hacker' branch in the intelligence or military has become the norm just like operating tank battalions. The occurring crisis on the Ukrainian-Russian border in the spring of 2022 has shown that cyber warfare is now an integral part of warfare in general as Ukrainian's critical infrastructure like banks and energy companies were targeted with hacking and disruption attempts (Sabbagh, 2022). State actors and big companies have one in common: they have the budget to maintaining cyber security operations centres, they can hire external pentesting and have a wide range of employees with specialised knowledge. At least in theory this gives them the tools to survive in a dynamic cyber space, but small businesses do not have these mentioned resources available to them (McAfee, 2020). Still, they are required to participle in an all connected, digital world. It is not feasible for a small law firm with e.g. eight employees to also run a dedicated Security Operations Centre (SOC) and a Computer Incident Response Team (CIRT) 24/7 (Santos, 2021, p. 22). This has the result, that small enterprises either lack necessary IT security or that they have to compromise on digital features for their employees and customers or they have to spend a lot of their budget on external service providers.

The Munich based consulting and managed IT service company IS4IT has a lot of small sized customers who are concerned with their information and IT security. When talking about security or any other topic in the IT industry a phenomenon has developed in the last few years: buzzword bingo. Buzzwords like quantum computing, blockchain, cyber or artificial intelligence have become

synonymous with the integration of digital products and content in our everyday life, private and industrial (IS4IT GmbH, 2022). And it has become a symbol of the disparity of actual technical know-how by CEO´s and just wishful thinking. When talking about security, the buzzword of choice is cloud. Many companies, whether small or big, have tried an all-cloud or could-first approach to their IT infrastructure, often driven by economical decisions and not operational or technical. Especially many German IT engineers and their leaderships regard cloud as a new IT security threat, they want to avoid (BSI, 2017, p. 4). The fact that many company leaders think about IT security is a good thing, for example 61% of small companies in Switzerland regard cyber threats as the biggest risk for their own enterprise (Mayencourt & Peter, 2021, p. 25). It has to be made clear that the cloud only adds new types of attacks while also adding features for security and usability. This thesis goal is to investigate if a cloud solution offers sufficient security and monitoring features for medium businesses so they can maintain their own IT security. The cloud solutions in question shall be the Microsoft Cloud, also known as Azure Cloud. With the popular service Office 365, Microsoft has established itself as biggest rival to the most popular cloud solution: Amazon Web Services (Davis, 2021, p. 20). The integration with widely used services like Microsoft Exchange Online and Office 365, Microsoft is especially interesting for small companies who would like to maintain a manageable number of suppliers. This thesis attempts to give an answer for technical decision makers whether the Azure Security suite is a practical and effective solution for securing small and medium companies.

1.2 ABOUT

1.2.1 THE AUTHOR

Paul A. Eisenmann is currently a student of Computer Science with the University of Applied Science (Hochschule für angewandte Wissenschaften) in Landshut, Germany. This thesis is written in the effort of obtaining the degree of Bachelor of Science. Mr. Eisenmann is a student at Landshut since the fall of 2019. He obtained his A Levels at the Berufsoberschule Freising. Before his A Levels he did a three-year apprenticeship at the media and television company ProSiebenSat.1 and finished his Computer Specialist for System integration apprenticeship in the top 2% range of all graduates in southern Germany. He worked part time as System Administrator for Windows and Linux Servers between 2018 and 2021. In this time, he was appointed IHK instructor and supervised fresh apprentices. Since Winter of 2021 he is employed at IS4IT GmbH as Junior Consultant for Microsoft

Cloud Solutions. At IS4IT he maintains his own customers, mainly in the healthcare industry, and supports this colleges with his scripting knowledge in several programming languages. He pursues his personal interest in cyber security in different customer projects or internally raised questions by other colleges. Mr. Eisenmann also holds a Certificate of Higher Education in Arts and Humanities from the Open University (Milton Keens, United Kingdom) and continues to pursue a degree in History. In the current term Mr. Eisenmann is head of the student representation in the faculty for Computer Science.

1.2.2 THE INDUSTRY PARTNER: IS4IT

Founded in 2022 the IS4IT GmbH is an IT service provider and consulting company that employs over 300 people with offices in Oberhaching, Berlin, Eschborn, Leinfelden-Echterdingen, Nürnberg, Obrigheim and Schwaig. IS4IT´s service focus lays on the following topics: user support, consulting, cloud solutions, workplace management, information security, and data centre operations (IS4IT GmbH, 2022).

The company's supervisor for the bachelor thesis is Mr. Nico Herpich. He is head of the Modern Workplace Consulting department and holds a Bachelor of Science degree in business computer science from the University of Applied Sciences Hof. Mr. Herpich is the direct supervisor of Mr. Eisenmann since November of 2021. His team currently has seven members with a wide range of skill set and different customers (IS4IT GmbH, 2022).

1.2.3 THE UNIVERSITY AND THE SUPERVISOR

The bachelor thesis is supervised by Univ-Prof. Dr.-Ing. Johann Uhrmann at the University of Applied Science. Dr. Uhrmann is professor for information security since 2016 at Landshut and as dean of studies in the deanery's board for the faculty of Computer Science (HAW Landshut, 2022).

Dr. Uhrmann earned his Diplom in Computer Science (comparable to a Master of Science) from the University of Applied Science in Landshut. He continued his studies with a Doctor of Engineering in Aeronautics and Astronautics in Neubiberg, Munich at the University of the Bundeswehr (German Armed Forces). Between 2012 and 2016 he was a member at the Munich based Siemens CERT team. His personal focus is on Linux security and cloud computing (Amazon, 2016).

Established in 1978, the University of Applied Science in Landshut as become a leader for higher education in Lower Bavaria. With over 5.000 students over six faculties Landshut offers a diverse range of taught academic programmes and maintains a range of industry cooperative research projects (HAW Landshut, 2022).

1.3 DEFINITIONS

1.3.1 SMALL AND MEDIUM BUSINESS (SMBS)

SMBs or SMEs (Small and Medium Business) are usually led by individuals and not shareholding companies. But their main characteristic lays in their name: they are small and usually located in only one country or region. In the European Union the definition for SMBs is set to less than 50 employees for small business and less than 250 employees for medium or midsized business. There are also limitations of annual turnover which shall not be taken into account for this technical thesis (European Comission, 2021).

Challenges for SMBs are often that one employee has several different responsibilities. For example, an IT administrator at a big company will be specialised to one topic, e.g., data storage, networks or Unix Servers. In a small or midsized company only a handful, often just one person is responsible for the whole IT infrastructure including user support which means that this person has to have a broad knowledge of different topics and they cannot be a specialist in every matter. Smaller businesses often contract manged IT service providers to help them with support and maintaining IT infrastructure. The extend of external help is often driven by cost not by actual business need (Mayencourt & Peter, 2021).

1.3.2 IT INFRASTRUCTURE

The thesis question is focused on existing IT Infrastructure. This broad term incorporates a lot of different components. This includes hardware like client devices (e.g., notebook, smartphone) or software components from operating systems, text editors to self-programmed applications. Also networking devices like switches and routers are part of the IT infrastructure. The RedHat organisation formulary defines is as “components required to operate and manage enterprise IT environments” (RedHat, 2019). Basically, anything digital in a business.

When it comes to different IT infrastructure type three different kinds can be defined. Traditional IT infrastructure or also called on-premise infrastructure means that all components are located at the company’s physical location i.e. their local data centre. Besides the location, everything is manged and owned by the organisation’s own employees. The opposite of on-premise infrastructure is cloud IT infrastructure. With cloud infrastructure there are still some resources that are the same as with a traditional infrastructure like user clients or basic network infrastructure (it is hard to virtualise a keyboard and still use it). The stark difference is in the data centre: the all-cloud approach does not have a data centre on location, but every server is virtualised with a cloud services provider. Popular cloud providers are AWS, Google Cloud, Alibaba Cloud, and the examined Microsoft Azure cloud (Irmer, 2018, p. 5). The third type is the combination of the first two. Some server applications make more sense to be on-premise (e.g. constant GPU heavy server application) then in the cloud due to cost issues. Also, legal requirements can disallow a transition of certain applications to the cloud. If only part of the data centre is moved to the cloud and some stays on-premise, it is called hybrid IT infrastructure. The cloud and on-premise network are connected with a secure channel i.e. VPN. The hybrid approach is the most feasible solutions for most cooperation (RedHat, 2019).

1.3.3 ANALYSING AND PROTECTION OF IT INFRASTRUCTURE

The IT security’s aspect of analysing IT infrastructure consists of multiple parts: the discovery and inventory of all IT assets, although this is more relevant for larger businesses it is also vital for SMBs to understand which assets have to be protected. The next step would be the monitoring of all assets, preferably with a centralised log collection. This would enable the business to detect any anomalies in the IT infrastructure which could point to an IT security incident. This solution is commonly known as SIEM (Security information and event management) where specific detection

rules can be defined to analyse certain patterns within the log data (Pohlmann, 2019, p. 29). Summed up, analysing IT infrastructure means to know, what is part of your infrastructure (and what is not), being able to collect log data and analyse this data to understand security incidents or wrong configurations.

Protecting is a very broad term, but in essence it means that the surface of attack is reduced and incoming attacks, from outside and inside of the network, are recognised and responded to. Protection of IT infrastructure is not only a technical challenge but also a personal because the employees have their fair share in protecting their infrastructure against malicious actions or wrongdoing by their colleges (Microsoft, 2022).

1.3.4 PRACTICAL SOLUTION

The raised question asks for a practical solution but what does practical even mean in this context for IT security and SMBs. The Cambridge Dictionary defines practical as “relating to experience, real situations, or actions rather than ideas or imagination” (Cambridge Dictionary, 2022). Applied to IT security this means that any measurements and guidelines have to be reasonable and possible to implement without major business interruption. As SMBs have only limited employee resources, the actions should not require specialist knowledge and should be understandable by basic technical personal or even non-technicians (Mayencourt & Peter, 2021, p. 17).

1.4 EXPLORING THE MICROSOFT AZURE SECURITY SUITE AND OTHER MICROSOFT CLOUD SOLUTIONS

1.4.1 DEFENDER FOR ENDPOINT

Microsoft Defender for Endpoint is the enterprise anti-virus solution in the Azure environment. If claims to fully integrate not only into Windows clients but also into Linux, macOS and mobile operating systems. It natively loges to a SIEM (see 1.4.2). Microsoft sales site notes these points as Defenders main features: centralized security management, attack surface reduction rules, device control, endpoint firewall, device-based conditional access, threat and vulnerability management, automated investigation with remediation and endpoint detection (Microsoft, 2022). It is important to note that Defender for Endpoint differs from the Microsoft Defender that is included with every customer Windows licence.

1.4.2 AZURE SENTINEL

With Sentinel, Microsoft introduced its first cloud-native SIEM (Security information and event management) and SOAR (Security Orchestration, Automation and Response) solution. The Microsoft advertisement promises it is „ your birds-eye view across the enterprise alleviating […] sophisticated attacks, increasing volumes of alerts, and long resolution time frames“ (Microsoft Learn, 2021). A SIEMs job is to centralise the storage of security relevant logs, events or other useful generated data that could be used to analyse the internal IT security (Mather, et al., 2009, p. 296).

1.4.3 INTUNE ENDPOINT MANAGER

The sales pitch Microsoft sets for Intune Endpoint Manager on its website is “Endpoint Manager meets organizations where they are in their cloud journey” (Microsoft, 2022). Its goal is to administer user, apps and devices from one single cloud dashboard. So-called Intune joined devices can fully be managed through the dashboard, this includes basic operational duties like restart or data wipe. It also is a software management and distribution platform where the IT administrator can create packets that are distributed to an assigned group. In terms of security Intune can create so-called attack surface reduction rules which can include disabling USB mass storage devices or URLs in PDFs. With compliance policies administrators can set rules that would alert the IT department if a

rule. e.g. a too old software version, would be violated. Intune works with Windows, iOS and Android (Microsoft, 2022).

1.4.4 OTHER PRODUCTS WORTH MENTIONING

Azure Active Directory is Microsoft´s cloud IAM solution and works alongside the traditional Active Directory service that can be found in many on-premise data centres. It manages users, computers and many more objects and resources (Cheshire, 2021, p. 214).

Microsoft 365 (M365) was previously named Office 365 and consists of the cloud version of the popular Microsoft Office suit that includes products like Word, Excel, PowerPoint and many more. The Exchange Online cloud e-mailbox is also used frequently and offers several security features integrated automatically (Microsoft, 2022).

Azure virtual machines are cloud based VMs that can be provisioned within seconds and are only billed on a usage and runtime basis. It can be chosen from several different operation systems including non-Microsoft ones. Azure VMs are scalable which means that the hardware resources available for each VM can be change dynamically depending on the workload (Cheshire, 2021, pp. 42-43).

1.5 LIMITATIONS

Trying to find a definitive answer to the question if an all-out cloud approach is effective for SMBs is a herculean task. There are so many possible angles to examine that several Ph.D.'s could be made about this question. Therefore, it is necessary to limit the expectation for a definitive, all-encompassing answer but rather see this thesis as a deep dive into several technical topics which are most important for technical decision makers in the SMB environment and maybe raise questions for cloud providers and science institutions for further product development or research into cyber security with the specific focus of vulnerable small and midsized companies.

The Microsoft Azure environment offers over 50 different services, a quiet few of them with security features or full security focus (Microsoft, 2022). Covering all security features of Microsoft Azure would not benefit this piece nor would it be helpful for SMBs, therefor the applications for examination will be mostly limited to the mentioned ones in 1.4.

It should also be noted that this analyse solely focus on the technical implementation, practicality from an administrator's point of view and the tools efficacy. Any cost related aspects, which are important topics that should be examined before any real-word implementation should be done, shall not be part of this thesis. To full examine the usability of the Azure Security suite this point should be investigated (see 3.3 Further points for research).

The thesis also limits itself to user end clients (Windows 10 clients) and standard server operating systems, but most real-world scenarios include specialised use cases, business processes or self-written programmes. Often these make up only a small part of any migration or inventory process in terms of size, but it takes considerably more time to cover any special case (Irmer, 2018). Also, mobile devices, i.e., iOS and Android devices, are nowadays essential for any business to keep being connected but they also shall not be a focus of this analysis. This also amounts to network hardware like switches and routers, any IoT (Internet of Things) devices like Smart TVs or gaming consoles and the developing trend of BYOD (bring your own device). BYOD means that employees can use their private devices for business tasks. The company's data is usually secured in containerised application, accessed with MFA via the browser or through an VPN connection onto a remote desktop server (Microsoft, 2022). Although interesting angles of research they shall be excluded from this thesis to concentrate on the main use case: standardized Windows clients.

2. INVESTIGATION

The initial question of this thesis, whether the Azure Security Suite can be a practical solution for SMBs, shall be investigated in two parts: in the first part typical cyber-attack will be carried out against a representative cloud test environment and past attacks from IS4IT customers who use the Microsoft Azure Security environment will be examined. Any personal data of customers will be reduced of this thesis in agreement with German and European legislation (BSI, 2017, p. 24).

2.1. EXAMINATION IN PRACTICE

2.1.1 CASE STUDY I: EXTERNAL ATTACK AGAINST NETWORK INFRASTRUCTURE

In the test the recognition and mitigation of network-based attacks from the internet shall be put to test while keeping the initial questions in mind: are the cloud tools practical and are they sufficient enough. This is what most people of the public understand when they think of hacking: some lonely guy in a dark basement gaining access to a remote system on the internet, in movies accompanied by a dramatic status bar and a lot of fast typing. Although external attacks against IT infrastructure are not like in the movies, they still pose a serious threat for businesses. In a traditional IT infrastructure setting, especially in smaller companies, the method of protection is broadly known - firewalls. Older firewall only allowed entry to specific ports or specific routes based on rules defined by ISO/OSI layer 2 or 3 (e.g., MAC, IP) (Santos, 2021, p. 30). Today every simple layer 3 switch (commonly known as “home router”) offers this kind of protection and bigger IT enterprises turn to so called next-generation firewalls. These firewalls offer features like deep packet inspection, this means the packet content can be analysed whether it could be malicious or if the connection was initiated from inside the network or from outside (Santos, 2021, p. 45).

Reducing the surface of possible attacks by reducing the amount of open IP addresses and ports to the internet has become industry standard for decades, but some services do require internet connection – the business cases that do not require any internet connection become more limited day by day. These services include webserver, mail servers and many more (Microsoft, 2022). If one of these services can be exploited by an attacker, he or she can maybe acquire full-access, so-called root access, to the compromised system and now they are inside the companies’ network. Some names that should be clarified here: a vulnerability is weak spot inside IT infrastructure component

(Engelhart, 2020, p. 214). This could be due to out-dated software or miss-configuration, but when there is no fix or patch, and the mitigation is unknown to the IT administrator to the vulnerability it is called zero-day vulnerability (Engelhart, 2020, p. 14). Although very rare, zero-day vulnerabilities are extremely dangerous. A current example for such a vulnerability is the Log4Shell incident in November of 2021 (Knop, 2021). When a vulnerability is used to upload malicious code, most commonly to secure the connection, it is called to exploit the vulnerability – standardised software packages are known as exploits. The uploaded malicious code is called payload (Engelhart, 2020, p. 349).

A standard that should be established in any IT department is called 'least privilege'. This means that every account, whether it be a service account or user account, should only have the right he does need for his duty and no more (Santos, 2021, pp. 235-236). In terms of workload for IT administrators it would be easier to just allow everyone full access because fine-lined access and authorisation policies are work intensive and require constant maintenance. This is an important topic to SMB IT administrators who have their hands full already. Although the consequences of an attacker gaining access to a company´s network that has least privilege in place and one that has it not, can quite differ in its damage outcome (Microsoft, 2022). The other point to minimize damage once an attack was successful is network segmentation which means that only server and client are in one logical network who have to be in one. The different networks are separated by firewalls and connection between them it monitored. For example, the employees' mobile phones do not have to be in the same network as the business' active directory server. In on-premise, non-virtualised IT environments this is a cost intensive task, but Azure offers some basic controls that can achieve network segmentation (Microsoft, 2022) (Cheshire, 2021, pp. 194-195).

2.1.1.1 ABOUT THE CASE STUDIES ENVIRONMENT

The case study is setup with a client acting as the attacker over the public internet. Thus, one server in Microsoft Azure has to have a public IP address. To avoid real damage to the IS4IT cloud environment the next step, gaining access to a vulnerable system in the cloud is simulated as deploying exposed and vulnerable hosts to the public should not be made in any case. From the infected host, further attacks are made against other component in the cloud. If an Azure ExpressRoute or Azure Site-to-Site VPN is in place it would also be possible to attack on-premise resources from inside the business network (Diogenes, et al., 2016).

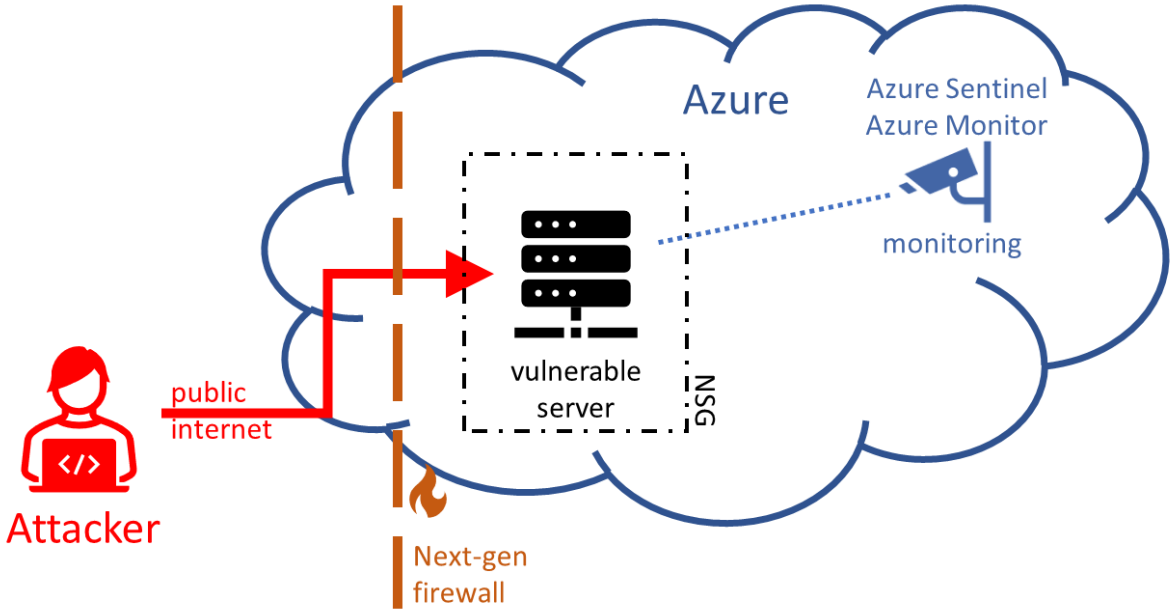


Figure 1: Setup for case study I

2.1.1.2 ATTACK DETECTION AND REMEDIATION

The main method of detecting attacks against infrastructure is through analysing event and security logs. This could include port range scans or IP ranges that were pinged numerical arising. Most traditional firewalls log these events, but they do not report potential malicious behaviour (Pohlmann, 2019, pp. 353-355). When configured correctly and with no open vulnerabilities there should be no need for logging this kind of attacks and target research but there is no guarantee of hundred percent safety. It is always possible that unknown vulnerabilities are be exploited. How vulnerabilities can be managed with the Azure suite is explored in more depth in 2.1.4 Case Study IV: Monitoring assets and vulnerability management. There it is also discussed how early detection of potential malicious scanning can alert IT administrators and maybe initiate a threat hunt inside the own network, whether the attackers were successful in gaining access or not.

In Microsoft Azure there are no firewall features that could substitute an on-premise firewall which makes sense as it is not reasonable to forward on-premise packets to a cloud firewall solution (Microsoft, 2022). This means that any on-premise network still needs a minimum standard of network protection, but for small business in most cases a simple layer 3 switch would be sufficient where internet access is handled, security logs are forwarded to a SIEM and where no server infrastructure is on-premise. When dedicated, on-premise servers shall be migrated to the Azure cloud

the service of Network Security Groups (called VPC in Amazon Web Service (Davis, 2021, p. 86)) has to be configured. These NSG are “the equivalent of a simple stateful packet filtering firewall” which means that they offer a basic set of firewall rules, mostly allow/deny rules and opening specific ports (Diogenes, et al., 2016, p. 56). The most important advantage of NSGs is that they are required for every server instance and therefor if they are configured correctly, a basic network segmentation, at least at ISO/OSI Layer 3 and 4, is achieved which would be much more cost-intensive in an on-premise environment (see Figure 5: Manage Network Security Groups). Azure also offers virtual next-generation firewalls that can be deployed for more precise network segmentation but frankly this is often out of scope for SMBs and maybe just interesting to separate a DMZ from the internet and the internal cloud network (Diogenes & Thomas, 2021, pp. 135-137).

A few other security related topics, not specific to cloud or hybrid environments, that should be noted in hindering network-based attacks and limit damage. Potentially exposed server like mail servers, webservers or any server in general should not run its service with root privileges. If an attacker should be able to remotely execute commands on a webserver this potential damage can be limited if the web server’s user has only very limited rights on the host server (Pohlmann, 2019, p. 244). Also, password should not be easily guessable, service accounts passwords should regularly be changed – this could be automated in combination with a password manager. Microsoft Azure offers the so-called PIM (Privileged Identity Management) “that enables you to manage, control, and monitor access to important resources in your organization” (Microsoft Docs, 2021). This means that if a potentially compromised account accesses an important Azure resources additional authentication, i.e. MFA, could be required and the action is logged dedicatedly (Microsoft, 2022). More on account and user behaviour shall be investigated in 2.1.5 Case Study V: Malicious employee behaviour.

2.1.1.3 CASE STUDY ANALYSE

The first case study has shown that cloud security does not really differ from traditional IT security. While Azure introduces new terms for old products the function remains the same. Most played through attacks were not mitigated because the network defence was a super-specialised cloud solution that solved every problem, it was rather that resources where misconfiguration or bad architecture planning came into play.

This first point is very essential for SMBs because often a single IT administrator has to administer the entire IT landscape, which means a single error when for example configuring a firewall could have devastating effects. This applies to cloud firewalls as it does to on-premise ones (Microsoft, 2022).

Thus, the effectiveness maybe could be measured by comparing the simplicity of configuring an Azure NSG to an on-premise firewall, but this creates an impossible challenge. Simplicity is a very subjective classification, e.g. an experienced on-premise Cisco firewall administrator would likely say that configuring a standard Cisco Catalyst is simple while being reluctant of the Azure NSG. So, this cannot be a valid measurement. A point that can be quantified is obligatory use. In an on-premise network a firewall is truly optional – no decant IT administrator would ever agree to this – but the reality shows that cost issues or in some cases knowledge issues lead to IT landscapes that lack basic security measures like missing firewalls, full open port ranges or no password protection (Irmer, 2018, p. 158). Although rare in this extend IS4IT experiences these cases in their initial assessment when customers want to migrate on-premise data centres to the cloud (IS4IT GmbH, 2022). When it comes to basic firewalls, no Azure IaaS product can be created without a NSG assigned – this does not mean that this NSG is configured correctly – but it requires or better said forces the IT administrator in question to think about basic access security (Cheshire, 2021, p. 195). A traditional on-premise server does not do this, and a traditional network is, especially in SMBs, not segmented, something that is far easier in the cloud environment. It should be noted that a cloud environment also introduces new threats like obtaining the global administrators credential which results could be devastating (Santos, 2021, p. 236).

The second point in question is whether SMBs should use servers after all. IT infrastructure also comes with a big overhead of extra work: this includes provisioning servers, updating, and maintaining them and monitoring them. Then services running on these servers often require high availability due to business needs which means that a fail-over must be configured – this requires specific skills by administrators, skills that many divisive SMB IT administrators cannot fulfil neither in an on-premise nor a cloud environment (Mayencourt & Peter, 2021). Thus, it may be better for SMBs to do not deal with these issues at all, after all an IT component you do not have is one that cannot be used against you. Of course, there has to be substitute for a traditional server and here PaaS or SaaS solutions can be a solution. This lays things like update and maintenance into the cloud solution providers responsibility – in most cases a big company like Microsoft who can afford a big Security Operations Centre – and relief the SMB with worrying about e.g. PHP emergency patches (Diogenes, et al., 2016, p. 8). This service often comes at a higher price point but is usually way cheaper than hiring an additional IT administrator. Regarding SaaS solutions there is also the advantage, that non-technical staff can use them, for example Microsoft Azure Web Apps lets you create web application without experiencing a single algorithms and data structure lecture or programming lesion in your entire life (Cheshire, 2021, p. 52). An important topic that remains with SaaS/PaaS solutions is

password management – here staff has to be educated about strong passwords and additional security measures, e.g. MFA, has to be implemented (Microsoft, 2022). A lot of Azure SaaS apps offer a direct security event connector to Azure Sentinel or Azure Monitor which is further investigated in 2.1.4.

To conclude this case study and coming back to the initial question whether the Azure security suite is suitable and practical for SMBs, the question´s answer in regard to network attacks is a simple: yes and no. In essence it is not a question of whether an Azure solution or an AWS solution is in place, and it is not a question of whether the IT infrastructure is in a cloud, hybrid, or on-premise environment. It is a question of implantation, monitoring and using security principals like least privileges, network segmentation and assume-breach. Those do not change with a cloud environment, in some specific points Azure makes things easier, e.g. network segmentation but in the end, it remains the IT administrator's knowledge and experience that ensures network safety. Thus, a redemption of traditional servers and a migration to SaaS/PaaS solutions can be a real time relief for overloaded SMB IT administrator. Such migration projects often require a short but intensive time expenditure, deep cloud, and business process knowledge. These points result that SMBs are often required to buy external consultant when such migration project should take place or existing staff has to be trained.

2.1.1.4 SUMMARIZATION

This first cast study has shown that cloud solutions are sometimes not even an option when talking about securing existing, on-premise IT infrastructure. It is simply not possible to virtualise a local switch or router or the company's internet connection. The attack attempts against the test-case server showed that it is not the cloud providers responsibility when an IT administrator did a bad job defining networking rules or forgot to update an old software version. So, the answer to the question whether Azure Security is practical for SMBs to protect IT infrastructure is yes but with a very big but. The real battle of secure IT infrastructure is fought with applying the right strategy: this includes the right mindset (assume-breach), the right configurations (know your environment and get external help if you do not) and keep a minimal standard for recourse you own (hard password, limited access, monitoring, …). So, it does not matter whether a SMB uses AWS tools, Azure tools or no cloud suite at all: it matters whether the SMB understood IT security in general.

2.1.2 CASE STUDY II: (SPEAR) PHISHING ATTACKS AND OTHER E-MAIL THREATS

In the second case study the emerging threat of phishing attacks shall be looked at and how the Microsoft Cloud offers security solutions to detect and mitigate these attacks. This example has to deviate a bit from the initial question: the question is about existing IT Infrastructure which was defined as on-premise servers. But Microsoft Exchange Online has now reached over 60% of all Exchange business which means it is more likely that a company has their mail service fully in the cloud or a hybrid solution in place mailboxes (Solution Mentors Inc, 2022). Therefore, this case study will look at a real-world example of a small company that has Exchange Online in use. Any data that could identify the company, an IS4IT customer, will be removed from any images.

The threat of phishing attacks has been a constant one over the last decade. It has to be differentiated between phishing mails that target personal or company data and spam or junk mails. Those are not as threatening as they mostly contain advertisement and hyperlink to dubious vendors (Schuh, 2020, p. 125). A typical phishing attack is started by an e-mail that is send to thousands of recipients. This e-mail is disguised as an e-mail from a trustworthy cooperation or organisation, e.g., Microsoft, Amazon or the Federal Bureau of Investigation (FBI). This mail contains either a hyperlink to a malicious website, that is also disguised as the real website, where the victim is asked to enter his or her credentials or payment information. The other option is that a malicious attachment is in the e-mail, often disguised as invoice, application, or any other important information, then installs or loads a virus, ransomware or trojan horse on the victim's client (Schuh, 2020, p. 127).

If a phishing attack becomes more sophisticated and targeting a single person or business, it is called spear phishing attack. This becomes extremely difficult to detect for human beings. A simple phishing mail can be easy to detect: no personal recipient address, awkward language or spelling errors or missing context (Pohlmann, 2019, p. 29). Assumed that the mail does not originate from a generic sender but from the victims boss name, mentions the current project name the team is working on and says a certain real-world contractor is in trouble and needs money imminently, the story often swings a different way and in favour of the attacker (Reischl, 2020, pp. 174-175). History has shown that it is not difficult to obtain this internal data with a few phone calls before the final attack, with the goal of obtaining money, is conducted. It may seem trivial on paper to notice that there is a spear phishing attack on going but put into the real-life situation it quickly gets hectic and emotional and any scrutinising of actions is stopped (DSBLS Inc, 2021). Thus, spear phishing is a huge risk for companies as it is hard to detect in the starting phase and even harder to protect once internal data and information is in attackers' hands.

2.1.2.1 ABOUT THE CASE STUDIES ENVIRONMENT

As phishing mails are one of the most common threats in today's IT environments real-world examples from IS4IT customers shall be used in this case study. Any personal data is redacted from the screenshot or data that could be used to trace back to the intended recipient. The IS4IT customers have Microsoft Exchange Online in place, some with a hybrid infrastructure to an on-premise Microsoft Exchange server.

2.1.2.2 ATTACK DETECTION AND REMEDIATION

It should be the final goal for anti-phishing solutions to block every incoming spam mail, but this would be unrealistic. If spam and phishing filters are configured to block every dubious e-mail, many legitimate, so called false-positive, e-mails would be put in Quarantine (Microsoft, 2022). This could have significant impact for the business processes and would be frustrating for employees. This means that besides technical solutions user awareness has to established to minimise phishing risk.

The Microsoft Security Center offers a feature called Probe Attacks with which a non-dangerous e-mail can be sent to specific users. If the employee does not recognize the threat and clicks the testing link, his action is reported to the Security Center and learning measure can be determined for the user, this could involve an educational video about phishing. For example, a fake Microsoft e-mail could ask for the users Office 365 credentials (Microsoft, 2022). The admin plane management view can be seen in Figure 6: Phishing Attack Simulation dashboard.

Nowadays most broad phishing mails are detected by Microsoft Exchange and therefore forwarded to the users' spam folder or hold back in Exchange Quarantine (Microsoft, 2021). User awareness is especially important for spear phishing attacks because mail content or senders' domains are created only for the purpose of targeting one company or employee. Now it shall be looked at the e-mails that are recognized by Microsoft Exchange as potentially malicious and the administrator's remediation options. The Exchange Quarantine page offers several remediation actions for mail administrators' seen in Figure 7:Exchange Online Quarantine dashboard.

For small operations without much external mail exposure the threat analysis offered by Microsoft Exchange Online may be sufficient but for larger organisations who have centralised security operations in place or who have external vendors operating their Security Operation Center (SOC) a connection to a SIEM would be recommended by Microsoft (Diver & Bushey, 2020, pp. 34-35).In 2.1.4

Case Study IV: Monitoring assets and vulnerability management the Microsoft SIEM Azure Sentinel is under investigation which would offer a native connector to Microsoft Exchange Online and there larger phishing campaigns could be detected easier which could trigger an internal workflow to warn employees about an ongoing campaign (Microsoft Learn, 2021).

2.1.2.3 CASE STUDY ANALYSE

After having a broad overview at the technical implementation is shall be investigated whether the solution offered by Microsoft 365 and Microsoft Azure are practical in the case of SMBs. The integration of the Exchange Online Quarantine into Microsoft Exchange is a single point of contact solution which makes administrative access easier. The reasons why mails are quarantined are clearly stated and comprehensible with basic IT knowledge.

On default settings users are not notified when mails are kept in quarantine which means that administrators have to regularly check the quarantine for false-positives or if employees are not receiving an e-mail they are waiting for, they need to ask their IT department for help. This could be an additional workload for an IT administrator who has already his or her hands full with other topics. Small businesses do not have the luxury to employ a full time Exchange administrator who can check Exchange Online's Mail flow on a daily basis or spend much time refining the companies spam policy for their specific business need. It is vital for a practical mail solution for SMBs to offer limited user self-services and limit the administrators´ time spend looking at a dashboard. These two points are areas where the Microsoft Exchange Online suite lacks potential but in regard to technical response to detect common spam, malware and phishing attempts the technical detection is state-of-the-art. A clear drilldown option for experienced administrators and option for forwarding to a (ITIL) ticket tool are important points it fulfils for a practical SMB solution (Microsoft, 2022).

This examination has shown that user training remains highly important to kept employees up to date on going and arising threats. Such training does not only work by talking about phishing mails, but it also has to be tested. Any simulated phishing attack to test users has to be done with the utter must subtlety because it could trigger negative responses from the employees, and it has to be made sure that no discrimination of employees takes place who 'fail' the test phishing mail and click on a link or open an attachment. Microsoft offers a phishing simulator for these test cases where a generic phishing mail can be created with a few clicks and send to a test group. If the user fails, the assignment and does not report the mail or even clicks the link in the e-mail the is offered to watch a video that explains the basics of phishing mails and how to spot them (Microsoft, 2022). Any such

actions are especially interesting for large organisations but due to the simplicity of the Microsoft dashboard it can also be a measure for SMBs to test their employees a few weeks after an information security workshop has taken place.

Mitigation of spear phishing is difficult because if it comes hard for human to differentiate between real and malicious e-mails it would be impossible for a (AI-supported) algorithm. Unfortunately, Microsoft does not publish in detail what it deems possible malicious but recommendations and warnings, in the same style of quick answers, would be an option to improve security if a mail includes a request for money or specific information. Otherwise, specific compliance settings in the Microsoft Compliance Center could be set that would trigger a compliance alert if sensitive information e.g., credit card numbers, social security numbers or custom non-public strings are shared with an external mail contact (Microsoft, 2022). Although these alerting options may minimise this risk partly it is a) very time consuming to implement and maintaining thus it is not worth it for SMBs and b) it only covers e-mail contact. Social engineering and spear phishing campaigns often use a combination of telephone, e-mail, and other communication channels (Reischl, 2020). Thus, spear phishing and the core essentials of information security are to be uphold by the employees – this job cannot (yet) be overtaken by technological solutions.

2.1.2.4 SUMMARIZATION

This second case study has proven why Microsoft Exchange Online has become one of the most requested cloud transitions that reach the consulting company IS4IT. Besides the not mentioned advantages of cloud mailboxes the here investigated security features are easy to understand and do not require intensive training. Most basic security related operation can be done by IT staff without Exchange Online specific knowledge, but it has been shown that administrative effort maybe increased if many e-mails are stuck in the quarantine, which could also trigger user frustration when it would occur. In regard to phishing, especially spear phishing, the backbone of every IT security measurement still remains the users. This is because phishing is not limited to e-mail but also involves telephone communication, traditional paper mail and any other human interaction. Therefore, continues employee training and awareness is essential to build a strong phishing defence. In this regard the Microsoft Security suite can offer tools for training, but it cannot replace a full information security compliance strategy. The technical options in Exchange Online are sufficient for SMB IT administrators in regard to superficial threat analyse and threat remediation.

2.1.3 CASE STUDY III: VIRUS PROTECTION WITH FOCUS ON RANSOMWARE

According to the United Kingdom's Cyber Security agency NCSC the threat of ransomware is currently one of the most severe. According to Sir Jeremy Fleming, the NCSC chief executive, "there was an increase in the scale and severity of ransomware attacks, targeting all sectors from businesses to public services." (NCSC, 2021, p. 12). Ransomware attacks have a simple goal: hold the attacked person or company at ransom. Usually this is done with the intension of financial gain whether it is through direct payment from the victim to regain access to their data or sell the obtained data on the black market (BKA, 2021). Nowadays it has become usual that attackers pursue both approaches and therefore gain two independent revenue incomes. The means of pressure is made through encryption of files, both locally and network stored data. This encryption is nearly impossible to break without the encrypt-key that the attacker trades in exchange of money, commonly in the form of nontraceable cryptocurrency with Bitcoin being the most widely known one (NCSC, 2021, p. 16). The entrance of ransomware is possible through any form where users can download or access software, this could be malicious websites, 'found' USB sticks and the most common one: e-mail. Once inside the network the malicious encryption software can spread to other computers, sometimes using exploits or more commonly shared network drives (Schuh, 2020, p. 132). Especially encrypting network shares can be extremely painful for business as they hold most of the companies' data that is required for everyday work. This means that encrypting several clients and shared data can, in the worst case, be threatening the company's existence. Famous examples of ransomware include WannaCry, Nyeta and NotPetya (Santos, 2021, p. 52).

SMBs are at very high risk of having severe ransomware attacks because they often lack the network protection like mail attachment inspection (Mayencourt & Peter, 2021, p. 55). Another problem is that due to administrative expenditure a lot of companies grant their employees full install access on their clients which means that ransomware can be installed in the first place. And finally, SMBs may not be aware of the increasing ransomware threat and are not educating their employees to be more cautious when interacting with mail attachment or any other unknown data. While the German federal police says that the ransomware threat is especially high for bigger businesses, the so-called big game, the impact onto SMBs is often more devastating for the business continuity. They also warn that with the appearance of Ransomware-as-a-Service (RaaS) the number of malicious actors will increase which means, that more targets, including SMBs, must face this threat (BKA, 2021).

2.1.3.1 ABOUT THE CASE STUDIES ENVIRONMENT

The testing example of this case study is client focuses. It shall be investigated if the Microsoft endpoint protection (see 1.4.1 Defender for Endpoint) will recognise the ransomware, whether it will stop it and what data is reported to the IT administrator. A Windows 10 client connected to Azure Active Directory shall be used for this case in the IS4IT testing environment. Any connection to company data is restricted to prevent any possible damages through the testing case. To further avoid damage a ransomware testing software by vendor KnowBe4 Inc shall be used and not a real ransomware (knowbe4, 2021).

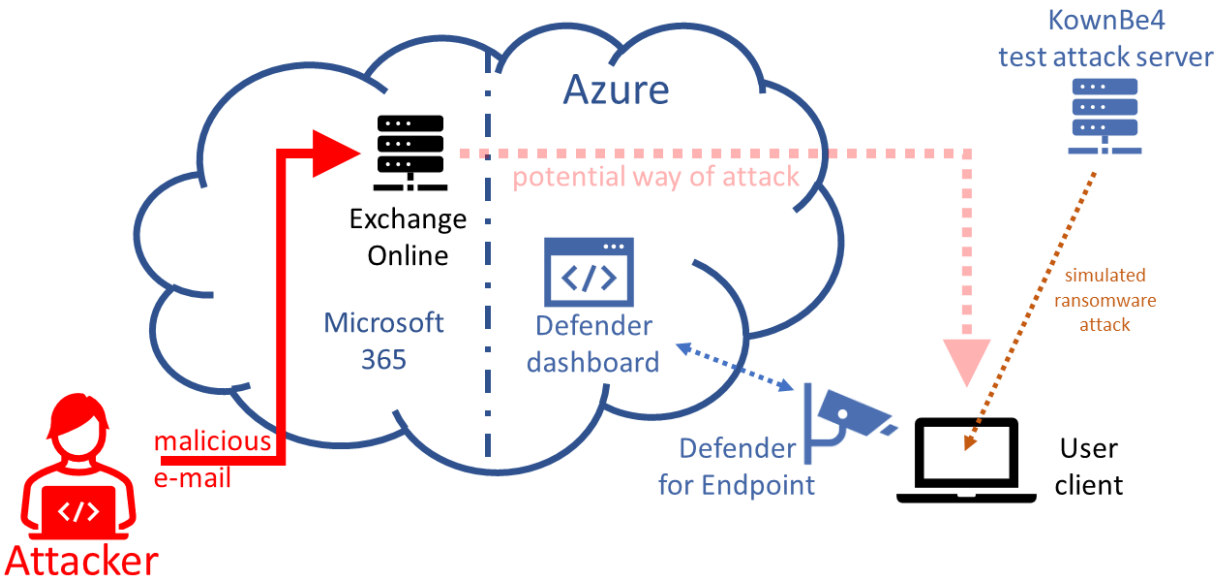


Figure 2: Setup for case study III

2.1.3.2 ATTACK DETECTION AND REMEDIATION

The best remediation of ransomware is to not even let it into any organisations network. This part was already partly investigated in 2.1.2 as e-mail poses the biggest entry point for executables and scripts that encrypt data. Although Exchange Online is quite through at detecting malicious attachments and many organisations do not allow receiving executable or script files at all, it is not impossible that a file falls through the loop (Diogenes, et al., 2016, p. 223). Although mail is a popular entry point others should also be looked at with browser download and malicious USB devices being other effective options for attackers. When scripts or internet links are hidden in the popular PDF file

format it can be hard to detect whether they are malicious so it can be advised for businesses to disable these pdf functions (Mayencourt & Peter, 2021, p. 49). In Microsoft Intune (see 1.4.3) the client option of surface attack reduction offers several features that are often exploited by attacks, that can be disabled companywide with a few clicks (see Figure 8: Attack surface reduction in Intune Endpoint Manager). Not granting the user install privileges on a client should also be a nonstarter as they are required for a lot of virus and ransomware to work. This does not mean that a user with no administrator rights cannot get his or her data encrypted it is just more unlikely – this is also one of the main themes of IT security: make attacks and damage as unlikely as possible (Pohlmann, 2019, p. 542).

If it is not possible to disable such functions due to business needs the final point of defence comes into play: Microsoft Defender for Endpoint. Generally, this product is known as anti-virus program and its product category has established itself as a common type of software in private and business environments. Most popular vendors are McAfee, TrendMicro, Kaspersky, and Norton just naming a few (Mather, et al., 2009, p. 32). It works by detecting program files hashes and detecting programs behaviour that could be fraudulent (Mather, et al., 2009, p. 44). In this test case, after launching the ransomware Defender imminently prompts the user that a malicious behaviour was detect by the executed program and that the program was stopped. This incident is logged to the Defender for endpoint dashboard where the IT administrator can see the incident in detail (see Figure 9: Dashboard Defender). There the incident is also enriched with public information that Microsoft has on this ransomware, possible mitigation, and further online information. When the attack occurred several times in the organisation the incidents are also clustered and a diagram of infected devices is shown (Microsoft, 2022). The action panel also shows advised action for incidents, that could include systems changes, new attack surface rules or specific device network isolation for further investigation (Microsoft, 2021).

Although the remediation of mail, network and client protection are sufficient for most cases it is not impossible, especially when a specific attack on one organisation occurs, that significant damage is done before the attack is detected and stopped (Cheshire, 2021, p. 128). Thus, there have to be a mechanism in place to restore data that is damaged, maliciously change or lost. This is better known as backups. These backups should not be connected to any user client or server as it would be pointless if during an attack the backup also gets encrypted. Although there are many third-party tools on the market that offer backups from cloud storage it is also possible with Azure to regularly backup any data from SharePoint Online, OneDrive, any virtual server or Exchange Online to a specifically protected ‘storage bucket‘ that cannot be change without having a specific backup password or the

data is even in another Azure tenant, increasing security even more (Diogenes & Thomas, 2021, p. 244).

2.1.3.3 CASE STUDY ANALYSE

The case study has shown that through several layers of security measures the ominous threat of ransomware can be minimised to an acceptable level. This threat minimisation is especially important for SMBs as they do not have the financial backbone of large companies to survive a weeklong IT outage or are able to buy new hardware for every employee if necessary. When using cloud resources, it is also very important to remind IT administrators that, although they do no longer have to worry about many operational topics, backups still remain vital to any information security strategy. Microsoft SharePoint's and OneDrive´s integrated backup functions have to be analysed in detail if they are sufficient for the organisation's requirement. User have to be sensualised, that e.g., only data in SharePoint or OneDrive is backup thus no company data shall be saved on local devices.

This case studies main focus was on Defender for Endpoint. The example ransomware was detected easily and very fast. The user was informed about the action comprehensible and the information for the IT administrator in the Dashboard was well enough enriched with information, that any IT administrator – not only cyber security experts – are able to understand the incident and take action. That is very important for SMB IT administrators although the tool offers more deep analysis options (i.e. "Advanced Threat Hunting") these are not the concern of most SMBs as the attack prevention is most important for them not a detail analysis and post-mortem analysis (Engelhart, 2020, p. 59).

In regard to the question of practical, the Defender for Endpoint with its integration into Microsoft Intune and the Azure Security Center plays well in its own eco-system of Windows clients. The deployment with predefined Intune packages and easy rule setup, especially the attack surface reduction, are easy and comprehensible measures that can be understood by non-expert of IT security only by navigating the Intune and Defender dashboard. Although the job is not done by randomly disabling any available feature in attack surface reduction because this could drastically hinder employees from their work. If it is made so hard that they circumstance company IT thus using non-monitored private devices, it could open up more security threats. This means that any feature removal has to be in accordance with business process, user requirements and it has to be communicated clearly to users. To also improve user acceptance the anti-virus solution should not impact client's performance. This was not tested in this case study but reports online suggests that on low-performant clients i.e., old models or tablet-pc's this can be an issue (Microsoft, 2022). Issues

arise when the step is taken outside of the Windows environment, as the best Windows anti-virus program is useless when a user gets his Android mobile phone infected with a ransomware that encrypts the users OneDrive from this mobile phone. These kinds of attacks are very rare and highly unlikely as app protection works differently on mobile operation systems compared to traditional desktop operating systems, but they are not impossible. So, a full-scale client protection has to view at every angle of user interaction with desktop, server and mobile devices.

2.1.3.4 SUMMARIZATION

To conclude this investigation into ransomware protection offered by Microsoft Azure and Microsoft Defender for Endpoint the test can be described as positive. Although the result usefulness is limited as new threats emerge with every hour and it is impossible to predict if Defender will detect these threats. The main conclusion that has to be taken from this third case study is, that only applying the Swiss cheese method of security can minimise the threat of any attack to a minimum: this means that several different methods should be used for protection (Pohlmann, 2019, pp. 29,33). Whether it be disabling scripts and external links in PDF´s via attack surface reduction, disallowing local administers rights for their clients or having an anti-virus e.g. Defender for endpoint in place. Only a combination of several measures will create a secure net that can face the cyber threat of the future.

2.1.4 CASE STUDY IV: MONITORING ASSETS AND VULNERABILITY MANAGEMENT

Responding and avoiding cyber threats is important but effectively monitoring existing assets is vital for detecting cyber-attacks. Monitoring IT assets is not only important for IT security but also for non-security related topics like availability and hardware failures (Santos, 2021, pp. 499-500). To the user or customer, it makes no difference whether the IT system is not available due to a cyber attack or due to a hard drive failure. Therefore, any IT Infrastructure should contain a form of monitoring and logging of important events. This monitoring system should also be able to send notification e.g., e-mails to IT administrators or service providers as a full-time monitoring of any software dashboard is not feasible. In regard to monitoring solutions, it is also important to define what is even part of the own IT infrastructure, although this problem is more common in bigger, more aged companies due to employee turnover or time there can be IT systems up and running in the server rack that nobody knows about (Mayencourt & Peter, 2021, p. 143). The same goes for client

devices as it should be clear on what devices company data is being used. This is especially important with BYOD clients, for example the best monitoring and data loss prevention solution (DLP) is ineffective if the companies boss works on an important spreadsheet on his weekends at home on his personal computer (Microsoft, 2022). If this computer got compromised and the data obtained by criminals, it would be nearly impossible for the IT administrator or investigators to follow up this incident or even know about it. This example should make it clear, that any monitoring solutions requires a clear assent definition in the first place to be effective. The Azure solution is question is called Azure Sentinel which can be classified as a cloud SIEM (Security Information and Event Management) (Microsoft, 2022). For more on Azure Sentinel see 1.4.2 Azure Sentinel.

The second topic of this case study is to test Microsoft Azures vulnerability management. The goal of vulnerability management is to scan your own IT infrastructure to detect any possible vulnerabilities on IT systems whether it be servers or clients. For Windows clients Intune Endpoint Manager (see 1.4.3 Intune Endpoint Manager) offers the option of defining compliance policies that every Intune joined client has to fulfil, this could be a minimal update version of the operating system, only allowed software installed, hardware security features enabled (e.g. TPM) or attack surface reductions in place (e.g. disallowing VBA scripting) (Microsoft, 2022). For server application the Qualys service implemented into Azure Sentinel can be used. This service is what is usually understood when talking about vulnerability management (Diogenes & Thomas, 2021, pp. 196-198). It´s job is to scan servers and if applicable clients for their software version and it checks these against known exploits. If an outdated server is detected where an exploit could do harm an alert is given to the IT administrator to respond to. As the vulnerability management database is regularly updated a continuing testing for common exploits is being offered. But vulnerability management only shows possible attack points - it does not prevent any attack (Pohlmann, 2019, p. 285).

2.1.4.1 ABOUT THE CASE STUDIES ENVIRONMENT

The test environment for this case study includes an outdated Windows Server in the cloud (it would also be possible with an on-premise server, but this solution was chosen for testing complexity reasons) and a vulnerable (TPM disabled) Intune Endpoint Manager joined Windows 10 client. The Microsoft SIEM for testing is a SaaS solution that has to be active in a Microsoft Azure subscription and thus does not require any provisioning. The Windows 10 client has to be provisioned as a Microsoft Intune device which usually requires an (recommended) operating reinstallation (Microsoft, 2022).

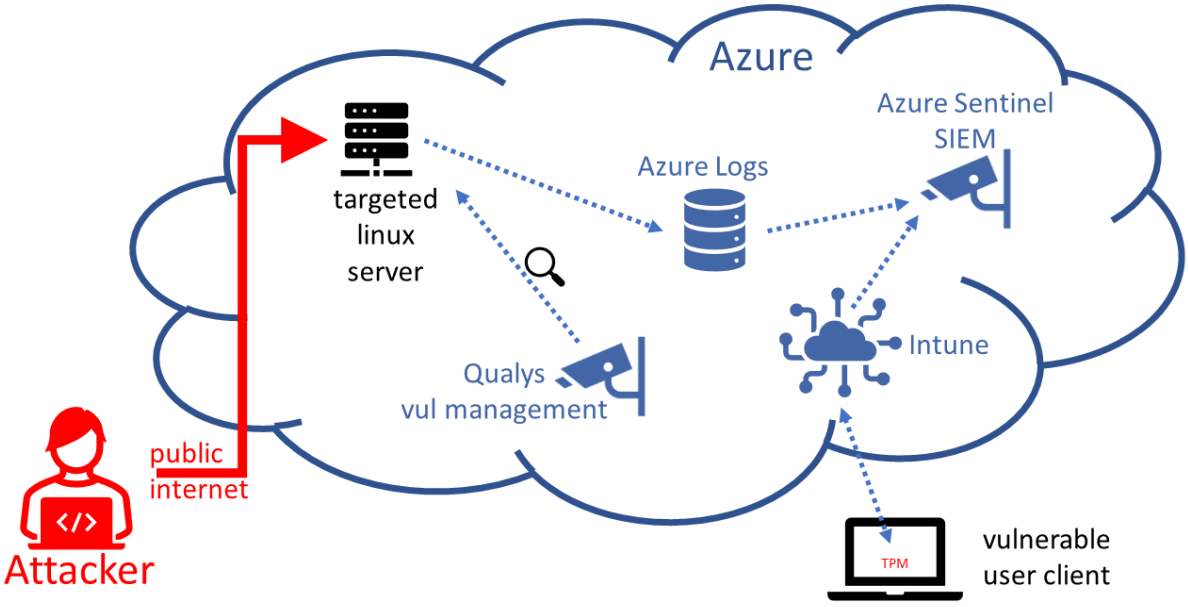


Figure 3: Setup for case study IV

2.1.4.2 ATTACK DETECTION AND REMEDIATION

Firstly, the possible vulnerable client should be looked at. The client is joined into the Microsoft Intune Endpoint Manager and thus compliance rules can be created for a group of clients or all clients of an operation system group (Windows, iOS or Android). To create a new compliance policy, rule the administrator can select an option from the predefined list, in this case ”Require Trusted Platform Module (TPM)” (Microsoft, 2022). There can also actions be defined in case of noncompliant behaviour. This could include rules defined in Azure Active Directory for conditional access e.g. a IT administrator can only log into the companies AAD account with a fully compliant, company device and MFA check. In this case study the compliance rule is just for alerting and monitoring and thus the example client is now visible as non-compliant. Intune shows which rule the client violates (Microsoft, 2022).

The vulnerability scanner solution of Microsoft Azure is provided by Qualys Inc and integrated into Microsoft Defender for Cloud (Diogenes & Thomas, 2021, p. 164). It is only available for Azure virtual machines and Azure Arc-enabled machines. With Azure Arc physical on-premise machines or virtual machines outside of Azure (e.g. AWS EC2 VMs) can be added to the Azure inventory and utilise Azure resources (Microsoft, 2022). Any alerts can be reported to Azure threat and vulnerability

management and custom rules can be created e.g. outdated software versions. For predefined alerts Microsoft supplies the administrator with recommendations on how to mitigate the issue, the vulnerabilities severity and possible business impact (Microsoft, 2022).

To understand the importance of a SIEM it has to be established what a SIEM is in the first place. When talking about SIEM solutions most IT security personal mean their SOC solution which includes two main components: the SIEM and the SOAR. SOAR stands for Security Orchestration and Automated Response (Santos, 2021, p. 381). Of cause a Security Operations Centre also needs solutions for vulnerability management, threat intelligence and incident response (Diver & Bushey, 2020, p. 21). The Azure Sentinel suite can be subdivided in three components: Azure Monitor collects data and does basic data analysis, Azure Sentinel is the core part where security incidents are detected and rules for incidents are defined and finally Azure Logic Apps which can be used for automatized incident response and remediation. So, to summarize, a SIEM is a log and event collection solution that analysis logs, detects IT security incidents by predefined rules or by AI-supported cases and then creates incidents for the IT security personal or initiates an automated remediation workflow (Diver & Bushey, 2020, p. 17).

In this case study the log connector was installed on the outdated server and had its logs forwarded to Microsoft Monitor (Azure Log Analytics Workspace) (Diogenes & Thomas, 2021, p. 179). On the test server the data forward logger was installed with a simple package. In medium sized companies it would be feasible to create predefined software packages with configuration details for the logger to simple install the logger onto new servers without configuration effort (Diver & Bushey, 2020, p. 69). The predefined connector was used to forward the data to Sentinel. In Azure Sentinel a test rule was defined that if there are more than five login attempts with the user handle root an incident shall be created. From an external client seven SSH login attempts with wrong passwords were indicated on port 22 and user root. An Incident was imminently created by the predefined rules. Defining the SIEM rule required three lines of Microsoft's KQL language which is similar to SQL (Microsoft, 2022). Sentinel offers predefined events that are logged, and recommendations are currently (2022) implemented. Azure Sentinel has a predefined connector for AWS CloudTrail that can be interesting for IT departments that use the best of Microsoft's (e.g., AAD, Exchange Online, Microsoft 365) and Amazons (e.g., AWS EC2, AWS S3, AWS Lamba) cloud world (Diogenes & Thomas, 2021, p. 217). As AWS is the cloud leader, it is likely that more IT administrators are trained with AWS than with Azure and this mimesis the vendor dependency on i.e., Microsoft. An Azure Sentinel dashboards example can be seen in Figure 10: Azure Sentinel dashboard

2.1.4.3 CASE STUDY ANALYSE

The investigated policies for Intune are easy to setup but knowing what policies to setup in the first place, can be a challenge. Here further recommendations, like the recommended actions in Microsoft 365 would be helpful for SMB IT administrators who are not IT security experts. Once a device is fully Intune-joined its management is easy and setting up cloud GPOs is much more comfortable than it is on a traditional AD server. Although the feature set is currently limited compared to an on-premise AD GPO set. The actions for non-compliant devices are a good improvement to relief IT client administrators in medium and big corporations but for smaller enterprises a manual intervention by the IT administrator would be more practical. The integration of mobile devices like iOS and Android devices is a great addition to combine full client management in one place and thus (probably) keeping company data more secure.

The Qualys vulnerability management add in for Microsoft Azure is a good addition for a full Security Operations Centre, but its desired role is questionable. The configuration effort and usability factors are too big for small corporations to consider implementation if not utterly required by regulation but the functionality and resources available in the implemented Qualys Azure version are not equivalent with the standalone Qualys service or other vulnerability management solutions on the market. Thus, raising the question what the targeted customer for this service is. From a practical point of view, it would be recommendable for SMBs to still consider vulnerability management but keep the effort to a reasonable standard. For example, an initial assessment by a service provider or an internal audit (requiring the internal know-how) combined with good asset management (see 2.2.1 ISO 27001 sufficiency) and strict update cycles can mitigate most vulnerability issues. Doing regular updates should not abolish any threat news monitoring e.g. the BSI threat newsletter.

The opportunities of Microsoft Sentinel are vast. As long there is a log file to analyse or any data exists about an incident, Sentinel can detect the incident within seconds. The emphasis has to be on can. If there is no predefined rule for an event it has to be created. The case studies example was simple but already required three lines of code – not much but any line of code for an SMB IT administrator is one too much, especially when thinking about future scaling. Most administrators will not be familiar with Microsoft KQL language which makes the first rules to define challenging and time intensive. If the first few rules do not work as intended the frustration will shortly set in. It also has to be noted that Sentinel is not as easy to understand as Defender for Endpoints dashboard which is much more straight forward. Looking up documentation for Sentinel is not just a quick Google search and for serious Sentinel setup the Microsoft documentations page has to be used which in its PDF version has adventurous 1898 pages (Microsoft, 2022). This cannot be called practical for SMBs. And

when lurking through the documentation it stands out how often the word ‘preview’ is seen. It is great how many features Microsoft currently implements in Sentinel that read great on paper, but this also means that dashboards, names, and documentation frequently changes and updates which makes it even harder for low-intensity users like SMB IT administrators. A feature of Sentinel that is ideal for SMBs is Sentinels payment structure because only the number of logs that are ingested into Sentinel are billed thus SMBs with just a few servers and e.g. a IAM application pay significantly less as a big cooperation with a whole data centre would (Diver & Bushey, 2020, pp. 31-33).

2.1.4.4 SUMMARIZATION

To conclude this case study this is the first case study that has shown great difference between big corporations IT security measures and SMB operations. SIEM solutions like Sentinel are great for a S&P500 business and not using such a tool would be negligent in today’s cyber world but the picture is different for SMBs. The initial and operational time commitment is so huge that the negatives overweight the positives for small businesses with one or a few servers. This can be mitigated when using a service provider for the SIEM monitoring and implementation but then it becomes a question of cost to benefit. The same can be said to vulnerability management for servers. In small IT infrastructures an initial analysis by an external service provider combined with maintained updates may be more feasible than a complex vulnerability management system. For user clients Microsoft Intune offers enough options and compliance rules to monitor a minimum standard of updates and checks for out-dated software. So, Sentinel is a great tool that is too complex for SMBs, and Microsoft Intune is a great option for SMB IT administrators to simplify their work while increasing IT security.

2.1.5 CASE STUDY V: MALICIOUS EMPLOYEE BEHAVIOUR

The finial point for examination is not an outside threat as it is feared by most IT security operators. So called insider threats have risen to 2500 internal security breaches per day in the United States alone (DSBLS Inc, 2021). Insider threats are security threats and incidents that originate from an authorised user or system and not from an external party (as in 2.1.1). This can include employees and third parties like IT contractors or service providers. Detecting an internal attack is much more challenging because it is difficult to differentiate between legitimate user actions and malicious behaviour. And an incident does not have to be malicious in nature it can also be accidental for

example a system misconfiguration or an inadvertent shutdown of a core IT infrastructure component. Such an incident would impact the IT security´s principle of availability but it can hardly be defined as attack against the company (Santos, 2021, p. 554). Malicious threat can be further subclassified into data theft, stealing company or customer information, sabotage, deliberately trying to harm the company's IT infrastructure, and finally espionage, which is like data theft but combined with the forwarding of information to company competitors. These high-stake cases that threaten company existence are not the majority of internal threats, that is properly data loss. 33 percent of employees in a recent survey stated that they would take internal information from their current employer with them if they would change their job (DSBLS Inc, 2021).

A threat that is not inherently an internal threat is compromised user accounts. When painting a worst-case scenario, the global Azure administrator for a SMB does not use a safe password and his or her account gets compromised by an attacker. Because the administrator in question is lazy, he also does not have multi factor authentication for his account enabled, thus with his credentials the attacker now has full access to all Azure resources but also to the Microsoft 365 application if the company uses them, like SharePoint Online or Exchange Online. Therefore, steps have to be implemented, that no one account that is used in daily administration has access to all resources and extra security measures have to be taken into account for users with special rights (Microsoft, 2022).

In this final case study, it shall be investigated how the Azure suite can detect and respond to malicious user behaviour. The two cases discussed in this investigation are a weak password by an employee with administrative access to the Azure environment and in the second step, one of the most dangerous scenarios: a full-scale deletion attempt by an internal administrator.

2.1.5.1 ABOUT THE CASE STUDIES ENVIRONMENT

The case study tests for two scenarios: credential theft and account misuse by an authorised and legitimate user. The first example is to test Multi Factor Authentication (MFA) and Conditional Access for Global Azure Administrators. This does not necessarily impact on-premise IT infrastructure, but most hybrid setups have shared credentials for cloud and on-premise resources thus once in the cloud environment the jump to on-premise resources can be easy (Microsoft, 2022). If a site-to-site VPN is in place misconfiguration or missing security check could also allow internal network access from anywhere in the world. The second scenario is a legitimate employee with cloud administrative rights who deliberately wants to harm the company's IT infrastructure.

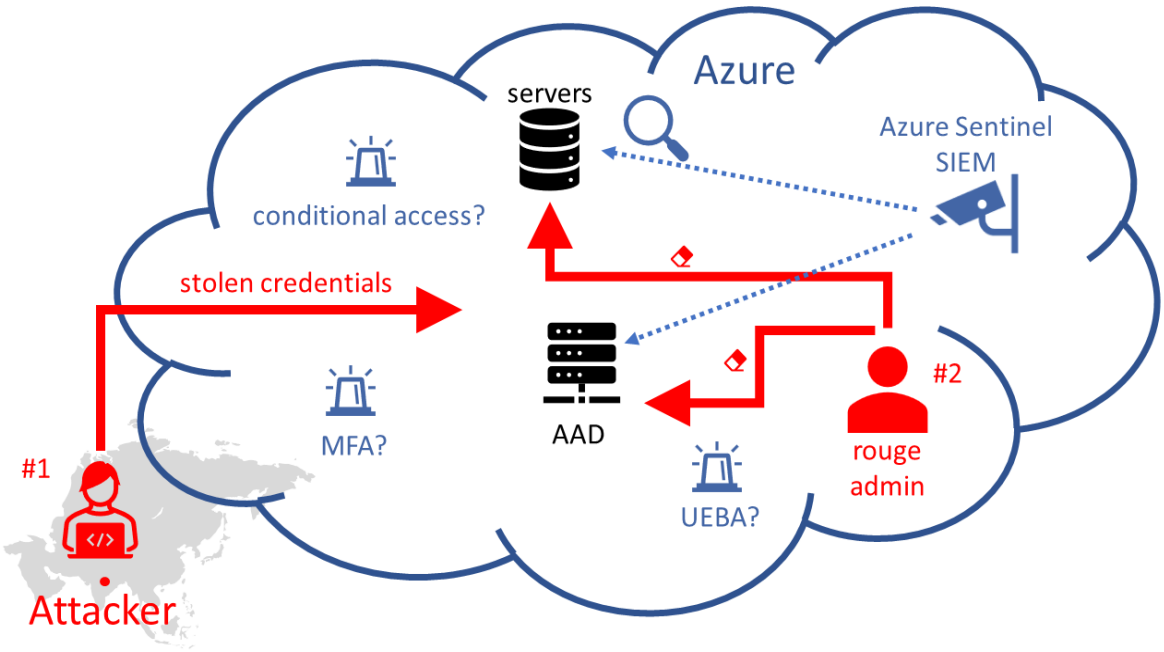


Figure 4: Setup for case study V

2.1.5.2 ATTACK DETECTION AND REMEDIATION

This last case study has to focuses more on detection and risk minimisation as it will not be possible to fully contain the risk of misused credentials. The first example is easy to solve. Businesses should never allow any administrative action without two factor authentication (Pohlmann, 2019, p. 188). This should not only apply to IT administration but also to any data manipulation that involves internal or personal data. MFA is also recommended for internal data access in general e.g., e-mails. The threat of example one is that passwords and usernames are guessable and thus the usage of usernames and passwords are not enough for important access credentials. This is complemented by the fact, that most users, even IT administrators, tend to use easy passwords that are related to their personal life (Irmer, 2018, p. 76). If rules for passwords are made strict, users tend to write their passwords down and leave them in reachable distance to their device which makes it easy for colleges or physical inducers to obtain. MFA mitigates this risk, but it is important to note that no MFA policy removes the need for strong passwords. In Azures Conditional Access MFA can be activated for every authentication or in this case for authorisation into the Azure administrative area. It is also possible to configure special rules that only allow administrative access from an internal network or that does not trigger MFA authentication (Diogenes & Thomas, 2021, pp. 46-47). In this example the 'attacker' was using an IP address from a country that the business in question does not do operate from thus blocking certain IP ranges from countries that the business identifies as hostile can be a solution that

should be implement. Although it has to be noted that it is for attackers as simple as it was for this case study to buy a good four US dollar VPN service and simulate a different location. Thus, geo-blocking alone is not a single option rather a possible piece of the greater puzzle of IT security (compare Swiss cheese model in 2.1.3' summarization) (Mather, et al., 2009, p. 152).

The second example is more about detection and not about securing infrastructure. This does not mean that network segmentation, least privilege and elevated rights do not matter but the reality in SMBs is that a few if not one IT administrator needs global or nearly global administrative rights to effectively do his job. In big IT departments, if the storage administrator goes rogue his damage should be limited to storage systems and does not impact the Active Directory server for example, but this is simply not possible in small businesses (Mayencourt & Peter, 2021). This means that alerting options should be considered that report unusual employee behaviour or that detect data losses. Microsoft 365 offers a Data Loss Prevention (DLP) solution that audits user behaviour and blocks possible data extraction outside of company (Microsoft, 2022). This only reduces data extraction risk as it remains possible to just take a picture from a monitor. Even if system monitoring (i.e., Microsoft Monitor, Azure Sentinel), DLP policies and Microsoft new User and Entity Behaviour Analytics (UEBA) is used, the damage that a single global administrator can do before he is detected or stopped is immense (Schmitz & Luber, 2020). Thus, backup solutions have to be in place for this risk and if possible, not every IT administrator should be able to delete them. When having full global administrative access, it was possible, even with all mitigation options in place, to fully delete the Azure resources inside the test tenant.

2.1.5.3 CASE STUDY ANALYSE

This case study has shown that it is not only important to implement secure technology but also intensively screen employees, especially IT administrators, and ensure that they are aware of their doing and their possible wrongdoing.

When going back to the point of not intentional internal threats the problems answer is quite simple and still very hard to implement: training. Most cases can be avoided when administrators know the consequences of their doing but the threat cannot be eliminated completely as long as humans operate there will be human error and it has to be calculated that sooner or later such a human error will occur. SMBs are much more threatened by this as big cooperation's. This is because of the multiple roles SMB administrator have to fulfil and thus they cannot be experts in every area of technology (Mayencourt & Peter, 2021, p. 23). Adding to this, due to many different IT responsibilities, in the

worst-case besides their normal non-administrative work, SMB administrators have to concentrate on many topics at once which could lead to being unfocussed and then making errors. It is therefore the leaderships' role to define reasonable workloads for their IT administrators.

The part of malicious employee behaviour should be mitigated by HR measures like regular employee talks, feedback rounds and an open business culture that keeps good employees inside the company and avoids situation that create such an anger that employees turn against their employer. As this is not a perfect world it would be irresponsible to assume that these measures would avoid every malicious employee behaviour and it is often not in the IT leaderships realm of possibilities to solve HR and general company issues. And it has to be emphasised that these problems are not limited to big cooperation's, but personal issues can arise in SMBs as easy or even more easily. In SMBs it is even harder to mitigate a personal situation like this because often all employees have to work together. Thus, it is the IT departments and administrator's role to take measures that minimise inside threats. This should include intensive training and warning of consequences if e.g. data is taken from the company as it is always a balance of limiting possible attacks and hindering users from their work (Pohlmann, 2019, p. 34). Having all important data on the user personal device is very practical for the user if he often has to travel but it is therefore also easy that the shows company information to his friend who happens to work at the rival competitor.

The Azure solutions in question are trying to face the threat of data loss and irregular behaviour but current state of the product cannot be called as practical and fully recommended for SMBs. This is due to many false-positive events which are no problem for a dedicated IT security department, but they create a not necessary workload for SMB administrators. To add to this, SMBs have not the same event frequency as big companies thus it would take even longer for the DLP policy to 'learn' what is considered normal company behaviour and what is not. Any measures that were already discussed in 2.1.4 i.e. monitoring asset status with a SIEM can lead to most high-risk internal threats (e.g., an alarm when several servers are shutdown or deleted at once) but it has to be considered that if the global administrator goes rouge he probably will first deactivate any alarms which creation he or she most probably supervised.

2.1.5.4 SUMMARIZATION

To conclude this final case study, it has to be noted that internal threats do not have the IT researcher's attention that they should have. Microsoft Azures attempts to face these threats is better than nothing, but these threats cannot be solved on a technical basis. It is the human component that

is in the sphere of control of the company in question. Thus, the main measures 'against' internal threats are training and good company environment. And in case of SMBs the technical measures to be limited to be reasonable which would include a SIEM, implementing least privilege and privileged access. One hundred percent security will not be possible, and this is especially the case with internal threats thus a special focus should be set on realistic risk assessment and recovery strategies e.g., backup and infrastructure as code.

2.2 EXAMINATION IN THEORY

The case studies in 2.1 have not only tested technical implementations but also asked question on things that go beyond hard- and software, mainly including the human component and business processes. Thus, in this section it shall be moved on from concrete Azure security tools to a broader, theoretical set of essays with three main topics: ISO's 27001 standard, problems in transition and considerations of IT experts. To fully understand theoretical concepts the conclusions and tools from the case studies shall be used to explain arguments raised in these three essays.

2.2.1 ISO 27001 SUFFICIENCY

Over the recent years it has become important to certify as a business and it is possible to certify for nearly everything. This trend has several reasons: standing out in a globalised business world and proving knowledge to customers being the main ones. One of the most important certification topics a business can or should gain is about information security – especially for business that deal with customers data. With the rise of cybercrime and with the media's attention about the GDRP (General Data Protection Regulation – European data privacy law) information security has gained broad focus in organisations and with company leaderships (BSI, 2017, p. 13). The standard that is spread around the globe is the ISO (International Standard Organisation) / IEC 27001 Information Security Management (ISO, 2022). Thus, it shall be this essay's role to test the examined cases studies in 2.1 and other features of Microsoft Azure and its security suit against the standard with a focus on small businesses. The ISO 27000 family of standards has so many risks and topics to cover that it would be impossible to cover all of them in this thesis, therefore some exemplary topics

have been picked to demonstrate a broader theme in the case of using Microsoft Azure from the viewpoint of SMB IT administrators.

2.2.1.1 ASSET MANAGEMENT

ISO 27001 defines asset management in its appendix A 8.1.1. as an important for archiving the standards goal (BSI, 2017, p. 49). What is meant by asset management? The first point is to know what assets even are in your IT infrastructure (BSI, 2017, p. 94). This seems logical and easy and for small enterprises it should be. Let's take a small business with nine employees and some basic IT equipment: this would include employee's mobile phones, Windows clients, a mail server – nowadays most likely already migrated to the cloud – and maybe a local server with an active directory, DNS, and a file share. On the network side it is unlikely that there is more than a switch and a basic router with firewall functionality. So, knowing that is part of such a small organisations IT equipment should be quite easy. When moving to the other spectrum of SMBs it is much harder to determine what is actually part of one's organisation. A medium sizes company with 250 employees is probably over a decade in business and had many different IT administrators, different IT equipment and different strategies in place. Thus, a mixture has grown over the years that no single person can know about, and it is not unusual that a totally outdated, old NAS is connected to a switch somewhere with no authentication in place. So how can the Azure cloud help with this and help managing assets better? In the case studies we have seen that the functions for on-premise hardware are limited and the real answer to succeeding in obtaining full company asset management is through company policy and by living information security – not a technical implementation. Although the Azure environment can help with achieving this goal. The most straightforward solution is of course a migration of on-premise IT infrastructure to the Azure cloud or any other cloud provider. This maybe a cloud consultants dream but it is sheer not possible or financially reasonable. In Case Study IV (see 2.1.4 Case Study IV: Monitoring assets and vulnerability management) Azure Sentinel and Azure Monitor was examined which would be a first place to see any server infrastructure in one´s organisation. This is only useful for a long-term overview of the equipment because if a server does not log to Sentinel there is no way of knowing that it exists. Using the vulnerability management scanning feature would be a better approach to manage the assets and have updates and maintenance task in view. This also would achieve ISO 27001 requirement for securing availability – one of the three pillars of IT security. Besides monitoring logs, it would be recommended that any server would be joined into the Active Directory (AD) or even better the Azure Active Directory (AAD). When a local AD is still in use a hybrid synchronization to AAD would be an option to use the same account in the cloud as for the on-premise

resources (Diogenes, et al., 2016, p. 25). Using the AD credentials would also offer options to log whether logon actions were authorised and, if the user has lost access right (department change), they can be deauthorised form a single source. This would be in accordance with ISO 27001 appendix A 9.2.6 (BSI, 2017, p. 51).

2.2.1.2 USER MANAGEMENT

Another topic that ISO 27001 covers is user management. In the first paragraph it was already introduced when speaking about the Active Directory. A.9.2.1 – A.9.2.6 requires that users are provisioned and deprovisioned, that every user has a personal account, a central management of privileged user accounts exists, that user privileges are regularly overhauled and a process is in place that removes and modifies user privileges (BSI, 2017, pp. 50-51). The topic of user management is also one of internal processes and technical implementations can only help a good process – a bad process will remain bad even if the most sophisticated management software is being used. A good user management process does not require a cloud solution like Azure Active Directory but when cloud resources are being used, starting with little things like Microsoft's Exchange Online, a single user management platform would be required. Especially for small organisations with minimal or no IT personal a migration to AAD would be interesting as a full AAD-joined company IT would not require an on-premise AD server and maintaining this server can be expensive. It should also be noted that a single local AD server is in conflict with ISO 27001 requirement for redundant systems (A.11.2.2) which are defined critical for the business operation (BSI, 2017, p. 52). This means to fulfil ISO 27001 at least two local AD server should be in place- maintaining them can get expensive very quickly. Although it should be noted that the AD's role can be defined as non-critical in certain business operations especially in business cases where the clients are not the main business tool of operation. The migration to AAD offers the SMB the advantage of 99.99 percentage guaranteed operational time, this is equivalent to ~ 53 minutes of downtime per year (Microsoft, 2021). The main challenge with migrating to AAD is defining so called Conditional Access rules for users and devices should be joined into Microsoft Intune, the application management solution of Azure. Implementing this change requires IT knowledge that is probably not present in a SMB IT department and therefore external help is required, but the advantages of such a migration are far reaching, especially if not existing software distribution and central management is in place. Intune offers administrators an option to centrally deactivate and erase client's data in security incidents e.g. client theft. It also reports clients operating system updates status back and software versions, thus policies can be created that when e.g., a critical security bug is found in Adobe Photoshop, the user is required to update the software

before he can access any company data again (Microsoft, 2022). With Conditional Access the ISO requirement of authorised user access can be improved: rules for impossible travel time (a login from the United States is impossible when the user just logged in from Germany two hours ago), unusual countries or a non-compliant/new device could trigger additional user authentication like MFA or a security alert for the IT administrator to check up on (Diogenes & Thomas, 2021, pp. 48,61). By setting up such rules there can be a good balance between ensuring user operability and their IT acceptance and providing ISO conform IT security. These features are not or only partly possible in an on-premise environment and can be seen as a worthy improvement. Further points in regard to user management in Azure that are noteworthy are PIM and the technical MFA implementation.

2.2.1.3 COMPLIANCE AND GOVERNANCE

As has been seen in the first to paragraphs, ISO 27001 is very much about process and not detailed technical implementation of certain systems. This is also the case for the horror spectre of most IT administrators: compliance, governance, and audit. Can Azure alleviate the administrators pain with these beloved topics? Firstly, what even is compliance: Cambridge defines it as “the act of obeying an order, rule, or request” (Cambridge University Press, 2022). And governance ensures that processes are in place that are effective and efficient while being able to achieve the business goals (Gartner, 2022). An audit is the evaluation and test of the compliance and governance measures in place with an outcome where room of improvement is (Harvard University). So, is this even relevant for SMBs? Yes, especially if an ISO 27001 certification is striven for and even if no certification application is planned the measures that are being set can be helpful for implementing a better information security and therefore securing one of the most important assets of 21st century organisations: data, knowledge, and information. Implementing a coherent compliance strategy can be seen expensive but the risks of losing data to avoidable reasons can be even more expensive for the business long-term operation. And the compliance measures only have to adhere to the business actual needs and the smaller the company the lower is the extent of compliance rules that are probably needed. One of the most commonly known requirements of ISO 27001 is document sensitivity classification. This can be easily implemented with the Microsoft Compliance Center, thus mails and any document in Microsoft SharePoint or OneDrive can be assign with a classification tag (ISO 27001 usually defines information with these four categories: for publication, internal, confidential and very confidential). It is also possible to assign certain policies to data that has these tags assigned – that would only be possible with third-party solutions in an on-premise set-up. An example policy would be that it forbids to forward very confidential tagged mails and documents to

external SMTP addresses (Microsoft Documentation, 2022). To be realistic, these policies that are set in the Compliance Center can be easily passed by thus it remains the job of compliance and the business leadership to define rules that are accepted and lived inside the organisation and not enforced by technical implementation. A security check that is bypassed, is not a security check. So, the augmentation continues in this third argument: Azure cloud can help implement more user-friendly compliance and governance controls, but it is not decisive in the information protection. The action talked about here require intensive IT training and education which can be a challenge for SMBs thus this challenge shall be investigated in more depth in 2.2.2 Exploring usability, transition, and maintenance problems.

2.2.1.4 TECHNICAL REQUIREMENTS BY ISO 27001

The final point of this short Azure cloud ISO 27001 implementation essay shall look into the more technical requirements that are set in appendix A of ISO 27001 and explained further in ISO 27002. After a deep look inside the requirements of ISO 27001 it becomes obvious very quickly that there are not much technical requirements set – why? Norms like ISO want to archive a business goal, i.e. archiving information security, and not to implement the most bleeding-edge Secure Hash Algorithm (SHA). The goal it sets out is to use “cryptography to protect the confidentiality, authenticity or integrity of information” (BSI, 2017, p. 113). When keep looking at cryptology, if older algorithms have some other advantages e.g., runtime and its security standard is sufficient it completely complies with the ISO norm. ISO 27001 for example requires for a key management and here Microsoft Azure can help to fulfil this ISO requirement. The norm explicitly asks for a guideline for the use during the whole lifetime of any key, this includes certificates, passwords, and private keys (BSI, 2017, pp. 114-115). It is important that Azure only delivers a solution for implementing the technical requirement of ISO 27001/2 not the policies and compliance requirements that come with it. The key management from Microsoft is called Azure Key Vault and Microsoft defines it as “a cloud hardware security module (HSM)” (Diogenes & Thomas, 2021, p. 281). In Key Vault any password, certificate or secret can be stored encrypted thus not even Microsoft can access the stored data. Every entry into Key Vault can be limited to a user group or a single user from Azure Active Directory (Diogenes & Thomas, 2021, p. 285). This is also a set requirement of ISO 27001/2: single point of administering user account, in this case if the AAD user is disabled he automatically is prohibited from accessing his data in Key Vault. This is especially important if an IT security incident is detected that involves a single compromised user account. Presumed the compromised user has a single account for every resource in Azure virtual machines, Azure Active Directory, on-premise servers, Azure Key Vault) it is likely that he would use

the same password/credentials for every account thus in the case of an incident it has to be investigated where the user is authorised, and every access has to be disabled manually. This is not only tedious, once finished the attacker probably already has done more than enough damage.

The ISO norm also defines guidelines for securely transmitting data over IT networks. The exact requirement is that "[t]he security of transmitted information, both within an organisation and with any external body, is maintained" (BSI, 2017, p. 141). This comes into place when any IT infrastructure component is moved to the cloud that should not be directly available to the public internet. For example, a database server that is used for an internal HR application and migrated to the cloud or even if only its logs are send to Azure Sentinel it is no recommended to send this traffic through the public internet. It has to be noted that any log connector should be encrypted but with old or self-made applications this can be a challenge. Thus, a secure connection between the cloud and the on-premise environment has to be establish in accordance with ISO 27001. Microsoft Azure offers two different solutions for this case: Azure site-to-site VPN or Azure Express route. Express route is a "dedicated WAN link between [the] on-premise location" to Microsoft Azure (Diogenes, et al., 2016, p. 81). The cost impact and the bandwidth this connection is overkill for SMBs thus the second option, Azure site-to-site VPN, is a more practical solution. With this site-to-site VPN the on-premise network is 'extended' to the set cloud networks. For the user the connected cloud server act like they are now in the local network and no connection to the internet has to be opened. Other scenarios are also thinkable with a site-to-site VPN, for example if the database server should remain on-premise but the logs and a webserver should be moved to the cloud. Therefore, a DMZ could be established inside the cloud, protected by always up-to-date, virtual next-gen firewall instances (Diogenes, et al., 2016, pp. 75-76). In conclusion, whether it be key management or network security, Azure offers basic protection that complies with ISO 27001 and would be more than sufficient to support business processes – but it does nor will it ever replace the need for implementing and living information security processes, it can only help to fulfil them.

These four paragraphs have painted a clear picture of Microsoft Azure security features and products. Even if only some topics were broadly looked upon, the message when it comes to compliance and governance is clear: security is first and foremost made by living it, not by buying the best software solution and implementing the hardest encryption algorithm. The talked about asset management and especially user management with Azure AD are an important improvement for any organisation that has no such solutions in place. Once committed to the Azure eco-system the central management prove comfortable to IT administrators, but it also locks an organisation to the vendor for many years and thus making the company dependent on the grace of Microsoft's price structure.

A challenge for SMBs who already have to turn every penny. Although to be realistic, many companies are already dependent on Microsoft's on-premise Active Directory so if any cloud recourse are used the move to Azure AD (or Azure Hybrid Connect) is nearly unavoidable if the business wants to be kept in accordance with ISO 27001 guideline for a single point of user management. The third argument has shown that once in the Microsoft eco-system there are many tools that can support the information security policies but the real extent that these are useful for very small companies is limited. The final part has continued with the main theme of this essay: the technology standard of Microsoft Azure, and also for Amazon Web Service, is more than sufficient for ISO 27001/2 as it is an additional component to look at or a supportive tool – but not the solution to the challenge of information security. The solution for this can only be the human component - from intern to CEO and without any weak links.

2.2.2 EXPLORING USABILITY, TRANSITION, AND MAINTENANCE PROBLEMS

Daring a move to the cloud with your security management and SIEM can seem like a hard decision, probably because it is one. Before considering such a decision there should be an intensive analyse in whether the product in question benefits the company´s business processes, whether it improves the company´s IT security and mitigates not acceptable risks and whether the own IT staff can implement and operate the solution in question. The case studies in 2.1 have shown only a short peak into the Azure security possibilities and they tried to test core problems, but different organisations have different needs that maybe very specific to the organisation and require punctual customised scripts. It has to be noted that customised scripts and any custom code is not recommended for SMBs if it is avoidable and rather use of-self solutions. This can minimise security loops and long-term maintenance issues that may arise. To investigate possible issues with Azure cloud security during migration and operation this essay looks at training staff, long-term maintenance and operational tasks and finally go full circle to the initial question and raise the question of usability and practicality of the Azure security suit.

2.2.2.1 EMPLOYEE TRAINING

The issue that was already touched on in 2.2.1 is very significant for small and medium sized businesses: employee training. With every new technology that is introduced into an existing IT infrastructure there are new software products the IT administrators have to learn. This is not limited to IT administrators, but also employees which creates an even bigger task for any software or hardware transition. In many but not most cases IT administrators are used to learn new products every half year or so, but common end users do not concern them self with new technology which makes any transition a challenge. This challenge can be faced by advertising the user that the transition or update includes new features which make their daily workday easier and more comfortable. In the case of a cloud transition, which automatically includes cloud security features, there are luckily many features which users can benefit from with world-wide access, improved uptimes and more collaboration features only being some of them (Cheshire, 2021). Especially in Germany a lot of users that are impacted by cloud transition project have similar concerns. Whether they are part of small projects like a SharePoint migration or big projects like a full data centre migration, IS4IT consultants are often faced with the same concern: data privacy. The thought that the company's or any private data is no longer in the own cellars data centre or NAS but in a remote data centre, managed by a global company can be frightening for many people. This can be due to fear of intelligence agencies like it was uncovered in the Snowden-PRISM leak in 2013 and with this there is always the fear of industry espionage (Greenwald & MacAskill, 2013). This means that internal company information, maybe company production secrets, are stolen by foreign, in the Azure case the United States intelligence services, and given to US companies to stay up to date. There is no real proof for this claim, but the cold war espionage has shown that nothing is impossible. Microsoft Azure claims that its data encryption can only decrypted by the data owners but there could be loopholed to go around the encryption – very unlikely but not impossible (Microsoft, 2022). This shall not take up any more space with claims that are not (yet) provable. When data privacy fears are alleviated both for administrators and users the actual challenge can be faced: training the company's stuff. In the case of Microsoft Azure there is a broad set of books and online learning resources available from Microsoft and third-party vendors, but it will not be met with much love if a company's leadership buys their IT administrators some books to read with the information to implement this 'cloud stuff' into their IT infrastructure. Thus, administrators have to be sent to human led trainings, but they can easily cost several thousand dollars for just a single person (Davis, 2021). So, any money that may be saved by a cloud transition is burned away by training thus making the transition not tantalising. It is therefore a practical way to slowly start experimenting with a cloud environment and do not try to do

a full cloud migration in one step. Going to the cloud, whether it is just security monitoring, user management or the data centre in general, is a process that can and in most cases should take several years thus spreading the learning gap for administrators and spreading the training cost for the leadership. This approach also improves user and administrators' acceptance for cloud features.

2.2.2.2 LONG TERM AZURE SECURITY MAINTENANCE

The next point that shall be looked at is maintenance of the Azure cloud security solutions. In a traditional IT environment maintenance of security solutions heavily dependent on the business size and the extend of solutions in place. In the worst case there is not much maintenance for IT administrators because there are no extended security solutions in place after all. It is not uncommon for IS4IT consultants to see companies, especially those with ten or less employees, with a non-business Layer 3 switch left in factory configuration, a wireless network setup with an easily guessable password or an old encryption method. A use of any cloud security recourse would of cause create additional workload for the IT administrator. Frankly speaking at this small company size the administrator would to the 'tech stuff' just beside this actual work thus making any additional time he or she has to spend on IT infrastructure a cost intensive burden for the business. The smaller the company the more important the billable employee times are and therefor time that is spent administering the own IT department is 'lost' at least in business administrating eyes (Mayencourt & Peter, 2021). To if a company that has not security measure beside a basic firewall and maybe an anti-virus software in place will experience that there is no cost or feature benefit from adding Azure security features like Sentinel or Defender for Endpoint. This fight between IT security responsible and leadership is nothing new, no matter how much is spend on IT security, no IT administrator can guarantee hundred percent security anyway, so some leaderships tend to cheap out on security or only are willing to invest when an incident is already occurring (Pohlmann, 2019, p. 18). This would be the same logic as trying to buy a fire truck when the building is already on fire. Once any budgeting concerns are overcome, the migration to Azure security has been taken place and the IT staff is trained there is still a lot of work to do. The best SIEM is no good if there is no employee responding to the events is created. The automated response features briefly mentioned in 2.1.4 in Azure Sentinel can automate a lot of incident types but there are still actions that require human interaction (Microsoft, 2022). Besides true incident alerts there is a good chance of false-positive detections, especially in the beginning of any SIEM implementation. This can create a challenge for user acceptance in the first weeks and months if the 'new' software that should make the IT administrators work easier actually creates more work – at least in the start-up phase. Even when these problems are solved there

remains a lot of work to in the long term. In the case of any SIEM new connectors have to be configured when new servers are introduced, and new detection rules have to be applied. With new security threats emerging every day there should also be a monitoring of any security related news e.g., BSI or NCSC security newsletters, and creating new rules if any new threat impacts the own environment (BKA, 2021). It is not only SIEM rules that have to be maintained, any good firewall needs regular inspection and the mentioned user privileges management in 2.2.1.2 also requires review that cannot be automated completely. Thus, it can be concluded that when thinking about integrating any new security feature the workload of the long-term maintenance has to be considered and not only the initial start-up phases work. Or formulated differently: security comes at a certain price, and it is worth this price as long as any security risk is high enough to justify this price.

2.2.2.3 MEASURING PRACTICALITY

The final point in question is usability for SMBs and why a cloud security approach is interesting, especially for SMBs. Usability comes back to the initial question of how practical the Azure security suit is. By this point technical and organisational pros and cons of Azure security have been investigated thus this point shall be put up to the challenge of their usability. Measuring usability is difficult but the main questions that shall be taken for this examination are: How long does it take to learn a certain Azure tool? Is there any on-premise solution that does the same job or does it better? Does any Azure cloud competitor, mainly Amazons Web Service (AWS), fulfil the same requirements or does it even better (Davis, 2021)? To fully investigate usability if should also be looked at the cost difference between on-premise and cloud solution but this question is not in scope of this thesis quest (Pohlmann, 2019, pp. 576-577). The first point of investigation was attacks against IT infrastructure which has shown that no cloud vendor has a solution for securing servers or even network components in an on-premise environment. The security features of the Azure security suite primarily focus on cloud environments with Network Security Groups being the most prominent feature in question. Amazon VPC feature works in a similar way that enables network segmentation with a few mouse clicks – a process that is much more intensive in an on-premise network as it requires multiple firewall instances (Cheshire, 2021, p. 197) (Pohlmann, 2019, pp. 330-331). It should be noted that this claim applies to non-virtualised IT architecture which becomes more and more uncommon. Virtualised data centre software vendors offer solutions that can create virtual firewalls with the same or even more advanced feature set that NSGs.

To conclude this short investigation into the problems that usability, transition and migration to an Azure security solution can create it can be said that everything stands or falls with user commitment. The first point of training employees and users only works smoothly when enough resources, meaning budget and time, is set available by the leadership and change benefits are clearly communicated to users thus creating an intrinsic motivation for users to adapt to new software and workflows. The second argument pointed out that once committed to a cloud solution the danger arises that a SMB cloud get dependent to the cloud vendor, and it was also discussed whether maintaining cloud solutions is more work intensive than on-premise one. And finally, the aspect of usability was looked at, but it was concluded that usability is such a personal opinion that no scientific result can be made in this technical analysis. Although in terms of IT security the measures and requirements set by Azure were considered an improvement to on-premise environments due to a minimum of forced security standard.

2.2.3 REAL WORLD CHALLENGES OF AN ALL-OUT CLOUD SECURITY APPROACH

The previous paragraphs and investigation have shown that a cloud security approach is heavily driven by policy and process implementation and not specific technical details what the Azure cloud is able to and what it is not. Therefore, it is the human component who is at the centre of any implementation or migration to an all-out cloud security approach or more broadly speaking to any migration at all. In the end, technology is there to enhance and help business processes not determine them. So, to include this human factor it is this thesis goal to incorporate issues and benefits that experienced IT security personal see with moving to a cloud security solution i.e., Microsoft Azure Security and Microsoft Sentinel. These very personal options will be enriched by conclusions from the case studies and other examinations of this thesis. This examination offers a narrow pick into the minds of leading security specialists as they are often in the role of convincing leadership boards that a certain solution should be bought and implemented. The question that was given to the following experts was left very broad because it was deemed interesting to see what these experts understood as an all-out cloud security approach.

The first expert that was questioned about a cloud security approach for SMBs is Mr. Damir Zelenbrz. Mr. Zelenbrz is head of information security at IS4IT and not only responsible for information

security topics at IS4IT but also consults IS4IT employees at their customer projects. His main focus is on compliance topics, especially the ISO 27000 standards. Mr. Zelenbrz describes himself as a cloud opponent as he has worked several years in the financial industry and therefore has reservations against (sensible) non-on-premise data. His main emphasis that is also supported by this thesis research (see 2.2.1) is, that technical implementations have to be chosen by a case-to-case analysis and no one-fits-all solutions can exists for SMBs. When it comes to data in the financial sector, patents, or so-called critical infrastructure (ger. KRITIS) cloud solutions, whether it be monitoring, or storage should be used with caution as it cannot be one hundred percent ruled out that Microsoft or intelligence agencies have access to cloud data according to Zelenbrz. The main threats that were named by Mr. Zelenbrz are also in accordance with the case studies: phishing, data loss (both technical and malicious) and e-mail related threats. He states that cyber threats for SMBs do not differ from threats that big operations face but this thesis has pointed out that both by threat type, IT infrastructure and employee capacity this differs. Especially when it comes to threat mitigation and response due to cost and workload issues the capabilities of SMBs are much more limited thus tools that were examined in the Azure suite that take of al lot of administrators work can be interesting for SMBs (see 2.2.2). The new feature of user and behaviour analysis was seen as a very positive development as he states that no on-premise solution can offer this integrated feature set and in his personal experience internal user threats are extremely hard to detect and pose a real threat to any cooperation. He also raised the issues of security acceptance as the stated “security always comes with a loss in comfort” but nevertheless the consequences of compromising on IT security would be worse. This thesis as shown that there are pathways that would introduce more comfort (at least for IT administrators) with cloud solutions being only a small part of automatization of IT infrastructure (see 2.1.2). Mr. Zelenbrz ended that interview with the note that information security has to be practised in everyday work and it is not something that lives only on process flow-charts and in highly sophisticated software solutions. Thus, he concludes, achieving information security with Azure and Microsoft 365 can be a practical SMB solution when it fits the businesses profile – but that is a case-by-case decision.

The second interviewee is Mr. Jonas Hilke B.Sc. He is consultant for Microsoft cloud products at IS4IT with a focus on the Microsoft 365 security suite. He notes that dependence on one big cloud provider can be a problem because the SMB is in the hands of Microsoft’s price structure. He adds to this, that the full security suite that he would recommend is very pricy and thus not a practical option for most small businesses. Although the Azure cloud offers solutions for SMBs that would not be in any range in an on-premise IT infrastructure like machine learning supported security software. Mr.

Hilke lays special emphasis on Microsoft's security dashboard that combines client, mail and server monitoring and incident management from one place which he notes is unique. Another risks he also identifies as it was seen in 2.2.2.1 is employee training and, if SMBs do not want to buy in expensive consultants they have to compete against the big players on the swept clean IT expert market. All in all, Mr. Hilke concludes that the Microsoft Azure product range is a good fit for a lot of SMB business cases, but it always should be a case-by-case decision and it has to be supported by good information security.

The third expert that was questioned is Mr. Fabian Neiser M.Eng., an IT security specialist at ProSiebenSat.1 (German TV station with around 5000 employees). Mr. Neiser does not have extensive knowledge in Azure security products but is an expert in technical cyber security and SOC operations. He states that operating a full-scale Security Operations Centre is not feasible for most medium to large enterprises. Thus, he suggests that basic monitoring should be favoured for SMBs and if a certain business need is identified, an external SIEM provider might make sense (see 2.1.4.4). Mr. Neiser notes that the usage of analytical user behaviour is especially problematic in Germany due to much stricter privacy laws, but he acknowledges that there are a lot of areas where an AI-supported monitoring could improve security. In regard to sensible data in the cloud and possible theft by intelligence agencies and cloud vendors Neiser states that "it is a question of paranoia" and when a cloud migration is planned there has to be a certain trust towards the vendors security promises. He adds that extremely sensitive data should maybe encrypted on-premise before being moved to a cloud storage. Overall, he sees more advantages for SMBs and especially start-ups in a usage of the cloud, but a full-cloud approach is always a case-by-case decision. The main cloud advantages he describes are easy fall-out prevention that would be extremely cost intensive in on-premise infrastructure and the scalability of (security) applications. To conclude he would recommend a serious proof of concept for any business that thinks about a cloud-first security approach that keeps business processes in focus.

To conclude these three interviews the main narrative of this thesis was confirmed that IT security whether for SMBs or big players is first and foremost a policy topic and only when looking at details the implementation, cloud vs. hybrid vs. on-premise, matters. This was also concluded for the case of Microsoft that if IT experts know the advantages of the cloud solutions offered, they can be deployed where they are practical and useful but non-cloud experts have difficulties to look through the cloudy range of cloud products on the market as its sheer number only offered by Microsoft is immense.

3. CONCLUSION

3.1. DISCUSSION

This thesis was started with painting a dark picture of the current and future state of small businesses IT security´s future. The numbers of daily cyber security attacks, the financial losses or horror stories where companies go out of business due to IT security incidences seem stunning for company leaderships around the world. It was this thesis mission to investigate whether the product range of cloud products by Microsoft can help SMBs in their challenge of surviving in a rapidly changing cyber market. SMBs limitations were always in focus of this investigation with practicality, easiness to understand and implement solutions and low training and maintenance efforts just being a few of the points that were important to consider. In the last decade, the move to the cloud was mostly limited to big corporations as they had the recourses to try such an adventure, but now small business also wants to profit from cloud computing benefits. Thus, cloud providers have to offer products that target IT administrators who are not cyber security experts while still keeping security at the necessary level to protect against a broad range of attack vectors.

In the case studies in this thesis five attacks that were deemed important to mitigate and understand were chosen to be tested against Microsoft Azures solutions in a SMB IT environment. The first case for investigation was the classics of cyber security: attacks against IT infrastructure over the internet. The example has shown that Azure does not offer anything besides monitoring for on-premise server and even in the case of cloud VMs it still is in the IT administrators' hands to configure the system properly. Once the attacker is on a system the cloud environment prevails against most on-premise environments due to easier network segmentation. Although this also needs proper configuration to be effective. The first example has set a precedent that continues throughout the entire thesis: without human checks there is no secure IT infrastructure possible not matter the product in use. The second example that was looked at was about phishing mails and how Microsoft Exchange can protect against those. It led to the conclusion that the simplicity of Exchange Online is a great fit for SMBs while still remaining a powerful tool against any e-mail threats. It was clearly visible that Exchange Online is Microsoft's cloud flagship product that should bind potential customers to Microsoft cloud solutions. The second case study has been in accordance with this thesis main message: when it comes to well-done spear phishing attacks no machine learning algorithms can spot the threat better than a good educated and trained human being.

The third case study has looked at anti-virus protection of user clients. While the virus detection itself is not a process in the cloud, the significant feature set of Microsoft Defender for Endpoint are located in the cloud environment. Especially the easy-to-use dashboard, the integration into the Windows operating system and the maintained low use were significant plus points for Defender for Endpoint. It was also explored how attack surface reduction methods can lower the initial risk of caching ransomware or any other malicious programmes and the full-scale integration with Microsoft Intune was deemed as a robust and comprehensive solutions for full range client management. Although the initial training expense to learn the environment was seen as not trivial. In case study four the focus shifted from the client to the whole IT infrastructure and its monitoring. The Microsoft cloud SIEM solutions was under brief investigation, and it can be said that it has evolved to be comparable to the big vendors like Splunk. The case study also concluded that monitoring one's infrastructure with a SIEM is very useful and recommended but it is not feasible for smaller organisations. Those organisations should think about investing in buying SIEM monitoring from external service providers who have the knowledge and capacity to run such a service. The final case study focused on an often overlooked attack: internal threats. The conclusion maybe disappointing for IT leadership boards as it was exposed that this threat can only be minimised and often has to be addressed by HR or good leadership itself. Implementing and living least privilege, establishing network segmentation, and monitoring elevated rights can point to possible misconduct of internal user accounts or lower the impact but this can be nearly impossible for small businesses. Thus, data backups and employee training still remain highly important in cloud environments.

To further question the practicality of the Azure security suite the thesis way of conducting the investigation shifted from a practical case study style to a more theoretical, process oriented one. The first topic under examination were issues raised by the ISO 27001 standard and how Azure security help achieving the standards guidelines. The essay came to the conclusion that the technical implementation of Azure is not decisive - it is decisive weather information security is lived on a daily basis in the business. Cloud offers a range of new possibilities of achieving the standards requirements while creating new challenge in IT security that have to be addressed. Thus, it is not possible to generally say if the Azure cloud security suite or any other cloud vendors suite is sufficient for a SMB. IT and IT security in general has to support the business process in the overall goal of producing, creating or however that business is making money. Businesses only should implement IT solutions that support their business, they should not be required to earn money to afford their supportive roles. Because that is IT after all: supportive. Thus, only IT security should be reasonable to the business needs and not be overkill. This was also explored in the second essay: problems and

challenges that may arise during the transition or implementation of Azure security into SMB IT infrastructure. Here the overall thesis credo was also visible that IT security is as much a technical topic as it is a business process topic. Training IT administrators and user on new software solutions can be expensive and time consuming thus it should be analysed thoroughly whether a solution is really needed. And it has been shown that IT security changes have to have the support of company´s leaderships and the IT departments. A move to the cloud should not be motivated by finical or business administrations incentives but rather a combination of business needs and technical features. The challenges of cyber security have gotten so broad that no single SMB IT administrator can handle all threats that the cyber space nowadays has to offer thus businesses should question how they can minimise their IT systems that need intensive IT security protection at all. It was mentioned that the move from on-premise or IaaS systems to a SaaS or PaaS solution minimises the administrators' responsibilities by a lot and thus making more free time to deal with ensuring a secure IT environment. Azure Active Directory served as a great example of how existing IT infrastructure can be moved to the cloud, new features be utilised, and old responsibilities abolished. This analysis was supported by leading IT security expert statements that were collected in the third essay and new issues that may require further solutions and investigations were raised like: European privacy laws, vendor dependency and business-oriented case-by-case decisions about a cloud approach.

To conclude this thesis there are three main take aways for SMB IT administrators and SMB leaderships:

1. The Microsoft Azure security suite has a lot of products to offer that are worth looking at, to improve any IT infrastructures portfolio. Most products in the area of IaaS and SIEM are nothing new and the offers by competitors differ only slightly. When it comes to Exchange Online, Azure Active Directory and its compliance and identity protection solutions Microsoft is way ahead of the market. These solutions are not perfect in any way, but they offer additional layers of security that are not available in on-premise environments or not that easy to set-up.

2. A decision for or against the cloud or Azure should still be meet by business need not by a convulsive attempt to migrate everything to the cloud. Although many offered Azure solutions are interesting to look at for IT security fans and IT administrators they may be overkill for small businesses or a simpler solution would do the job for less time and budget commitment. Thus, IT security and cloud security decision should only be driven by risk and need not yearning.

3. Successful IT and information security is not made by technological choices but by humans. Whether it be misconfiguration due to bad training, useless business processes or wasting IT administrators' times with questionable tasks. The best IT security solution is worthless when the employee has to work around it to fulfil this work efficiently. IT security, not matter if in the cloud, hybrid or on-premise, therefore has to minimise risk while still empowering employees with good IT infrastructure from mobile client to distributed data centres. This need has to be recognised by SMB leaderships and lived in everyday work down to the last employee as any information security system is just as strong as its weakest link.

3.2 LESSONS LEARNED

This thesis was set out to be a technical analysis of Microsoft Azure products, but the broad formulated question quickly showed that a serious attempt to answer it must involve a lot of business process questions while not losing focus of technical implementations. IT security does not work without the human component, thus involving it has been shown as vital in this text piece. It was deemed as very positive on how easy the Azure products were to use but when talking to IT industry leaders it was shocking how little many IT leaderships and IT security experts knew about cloud security products and it was also astonishing that academical research on cloud and SMB IT security was limited to non-existence. As it was clear that the detailed technical case study analyses were not directly helpful in answering the thesis question the decision was taken to focus on answering the main question not documenting the pen testing cases in much detail. This thesis raised more questions that it could answer thus IT security research that is focused on SMB and private individuals should not only be concocted by finically motivated corporations but a broader focus in academic should be put onto the human component of IT security. No matter how good the IT security product was if used by uneducated or misinformed personal its usefulness was near zero thus information security should have a broader focus in the public debate of IT security and how we conduct business after all. Another point to add is Microsoft naming strategy of its Azure products. Tools are so short-lived that names are nearly change on a yearly basis, some names sound similarly but the tools are not, or products are combined by a new name. This made it difficult to research written primary sources as the same tool could be named by as much as three different names. If this is confusing for IT security researchers, it would be sheer impossible for overworked SMB IT administrators to fully comprehend the Azure tool suit. It was also learned during this thesis that a typical IT administrators focus on desktop client for

security is an outdated concept because the users and the market is more mobile-first oriented than it is traditional client focused thus creating new challenges for IT administrators that were not properly addressed in this thesis.

3.3 FURTHER POINTS FOR RESEARCH

As previously stated, the thesis created more questions than it answered this includes questions of mobile SMB IT security, practicality questions of SIEM integration for SMBs, cloud based virus protection and detailed studies of Microsoft Exchange Online´s phishing and virus protection. The most important question that has to be answered for SMBs, so this thesis conduction has any value, is the question of money. The field of Business Computer Science should investigate the cost investment that would be required to a) implement a cloud-based security monitoring and client administration solution and b) migrate from an existing and diverse on-premise, time-grown IT architecture.

4. APPENDIX

4.1 REFERENCES

Amazon, 2016. *Amazon.de.* [Online]
Available at: https://www.amazon.de/-/en/kindle-dbs/entity/author/B01A5S2VFI
[Accessed 03 Januar 2022].

BKA, 2021. *Cybercrime - Bundeslagebild 2020,* Wiesbaden: Bundeskriminalamt.

BSI, 2017. *IT-Grundschutz Arbeitshandbuch.* 2nd ed. Colone, Germany: Bundesanzeiger Verlag.

Cambridge Dictionary, 2022. *practical.* [Online]
Available at: https://dictionary.cambridge.org/dictionary/english/practical
[Accessed 02 January 2022].

Cambridge University Press, 2022. *Cambridge Dictionary.* [Online]
Available at: https://dictionary.cambridge.org/dictionary/english/compliance
[Accessed 03 Febuary 2022].

Cheshire, J., 2021. *Microsoft Azure Fundamentals.* 2nd ed. Hoboken, NJ, USA: Microsoft Press.

Davis, N., 2021. *AWS Certified Cloud Practitioner.* Wroclaw, Poland: Amazon Self-Publishing.

Diogenes, Y., Shinder, D. T. W. & Shinder, D. L., 2016. *Mircosoft Azure Security Infrastructure.* Redmond, WA, USA: Mircosoft Press.

Diogenes, Y. & Thomas, O., 2021. *Microsoft Azure Security Technologies.* Hoboken, NJ, USA: Pearson Education Inc..

Diver, R. & Bushey, G., 2020. *Learn Azure Sentinel.* Birmingham, UK: Packt Publishing.

DSBLS Inc, 2021. *Insider Threats In Cybersecurity: How To Optimize Internal Security For Your Business.* [Online]
Available at: https://www.dsbls.com/resources/insider-threats-in-cybersecurity/
[Accessed 02 March 2022].

Engelhart, M., 2020. *Hacking & IT-Security für Einsteiger - Der leichte Weg zum IT-Security-Experten.* Berlin, Germany: BMU Media GmbH.

European Comission, 2021. *Internal Market, Industry, Entrepreneurship and SMEs.* [Online]
Available at: https://ec.europa.eu/growth/smes/sme-definition_en
[Accessed 22 Februar 2022].

Fornes, T. & Satterfield , M., 2021. *Mircosoft.* [Online]
Available at: https://www.microsoft.com/security/blog/2021/02/22/what-we-like-about-microsoft-defender-for-endpoint/
[Accessed 17. Februar 2022].

Gartner, 2022. *IT Governance (ITG).* [Online]
Available at: https://www.gartner.com/en/information-technology/glossary/it-governance
[Accessed 02 Feburary 2022].

Greenwald, G. & MacAskill, E., 2013. *NSA Prism program taps in to user data of Apple, Google and others.* [Online]
Available at: https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data
[Accessed 29 January 2022].

Harvard University, n.d. *What is an Information Technology (IT) audit?.* [Online]
Available at: https://rmas.fad.harvard.edu/faq/what-does-information-systems-audit-entail
[Accessed 02 February 2022].

HAW Landshut, 2022. *haw-landshut.de.* [Online]
Available at: https://www.haw-landshut.de/en/university/about-us.html
[Accessed 22 Februar 2022].

Irmer, U., 2018. *Cloud Security Grundlagen.* Norderstedt, Germany: Books on Demand.

IS4IT GmbH, 2022. *IS4IT About us.* [Online]
Available at: https://www.is4it.de/de/ueber-uns/
[Accessed 22 March 2022].

ISO, 2022. *ISO/IEC 27001 - INFORMATION SECURITY MANAGEMENT.* [Online]
Available at: https://www.iso.org/isoiec-27001-information-security.html
[Accessed 17 March 2022].

Knop, D., 2021. *heise: Kritische Zero-Day-Lücke in Log4j gefährdet zahlreiche Server und Apps.* [Online]
Available at: https://www.heise.de/news/Kritische-Zero-Day-Luecke-in-log4j-gefaehrdet-zahlreiche-Server-und-Apps-6291653.html
[Accessed 24 Feburary 2022].

knowbe4, 2021. *RanSim.* [Online]
Available at: https://support.knowbe4.com/hc/en-us/articles/229040167
[Accessed 30 November 2021].

Mather, T., Kumaraswamy, S. & Latif, S., 2009. *Cloud Security and Privacy.* Sebastopol, CA, USA: O'Reilly Media Inc.

Mayencourt, N. & Peter, M. K., 2021. *IT-Sicherheit für KMU - So navigieren Sie Ihr Unternehmen sicher durch Cyber-Turbulenzen.* Zurich, Switzerland: Ringier Axel Springer Schweiz.

McAfee, 2020. *businesswire.com.* [Online]
Available at: https://www.businesswire.com/news/home/20201206005011/en/New-McAfee-Report-Estimates-Global-Cybercrime-Losses-to-Exceed-1-Trillion
[Accessed 17 Februar 2022].

Microsoft Docs, 2021. *Microsoft Documentation - What is Azure AD Privileged Identity Management?.* [Online]
Available at: https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure
[Accessed 24 January 2022].

Microsoft Documentation, 2022. *Get started with sensitivity labels.* [Online]
Available at: https://docs.microsoft.com/en-us/microsoft-365/compliance/get-started-with-

sensitivity-labels?view=o365-worldwide
[Accessed 10 March 2022].

Microsoft Learn, 2021. *Exercise connect data from Azure Active Directory to Microsoft Sentinel.* [Online]
Available at: https://docs.microsoft.com/en-us/learn/modules/monitor-maintain-azure-active-directory/4-connect-data-from-azure-active-directory-to-azure-sentinel
[Accessed 23 Februar 2022].

Microsoft, 2021. *SLA for Azure Active Directory (Azure AD).* [Online]
Available at: https://azure.microsoft.com/en-us/support/legal/sla/active-directory/v1_1/
[Accessed 12 March 2022].

Microsoft, 2021. *Take response actions on a device.* [Online]
Available at: https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/respond-machine-alerts
[Accessed 30 January 2022].

Microsoft, 2022. *Create, test, and tune a DLP policy.* [Online]
Available at: https://docs.microsoft.com/en-us/microsoft-365/compliance/create-test-tune-dlp-policy?view=o365-worldwide
[Accessed 21 March 2022].

Microsoft, 2022. *Microsoft Defender for Endpoint.* [Online]
Available at: https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint?view=o365-worldwide
[Accessed 29 January 2022].

Microsoft, 2022. *Microsoft Documentation Sentinel.* [Online]
Available at:
https://opdhsblobprod01.blob.core.windows.net/contents/4a6d75bb3af747de838e6ccc97c5d978/e9055ce6477a768d1f6d619f47749650?skoid=2d004ef0-5468-4cd8-a5b7-14c04c6415bc&sktid=975f013f-7f24-47e8-a7d3-abc4752bf346&skt=2022-03-21T02%3A52%3A21Z&ske=2022-03-28T02%3
[Accessed 23 March 2022].

Microsoft, 2022. *Microsoft Endpoint Manager.* [Online]
Available at: https://www.microsoft.com/en-ww/security/business/microsoft-endpoint-manager
[Accessed 12 March 2022].

Microsoft, 2022. *Microsoft.com.* [Online]
Available at: https://azure.microsoft.com/en-us/services/microsoft-sentinel/#overview
[Accessed 06 March 2022].

Microsoft, 2022. *Simulate a phishing attack with Attack simulation training in Defender for Office 365.* [Online]
Available at: https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/attack-simulation-training?view=o365-worldwide
[Accessed 12 March 2022].

Microsoft, 2022. *Troubleshoot performance issues related to real-time protection.* [Online]
Available at: https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/troubleshoot-performance-issues?view=o365-worldwide
[Accessed 17 March 2022].

Microsoft, 2022. *What is Azure Arc-enabled servers?.* [Online]
Available at: https://docs.microsoft.com/en-us/azure/azure-arc/servers/overview
[Accessed 20 03 2022].

NCSC, 2021. *NCSC Annual Review 2021,* London: National Cyber Security Centre of the United Kingdom.

Pohlmann, N., 2019. *Cyber-Sicherheit - Das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung.* Wiesbaden, Germany: Springer Verlag.

RedHat, 2019. *What is IT infrastructure?.* [Online]
Available at: https://www.redhat.com/en/topics/cloud-computing/what-is-it-infrastructure
[Accessed 14 January 2022].

Reischl, G., 2020. *Internet of Crimes.* Munich, Germany: Reline Verlag.

Sabbagh, D., 2022. *The Guardian.* [Online]
Available at: https://www.theguardian.com/world/2022/feb/16/ukraine-accuses-russia-of-cyber-attack-on-two-banks-and-its-defence-ministry
[Accessed 21 Februar 2022].

Santos, O., 2021. *Cisco CyberOps Associate.* Hoboken, NJ, USA: Ciso Press.

Schmitz, S. & Luber, P., 2020. *Security Insider - Definition User and Entity Behavior Analytics (UEBA) - Was ist User and Entity Behavior Analytics (UEBA)?.* [Online]
Available at: https://www.security-insider.de/was-ist-user-and-entity-behavior-analytics-ueba-a-983974/
[Accessed 20 March 2022].

Schuh, J., 2020. *Cybercrime.* Heidelberg, Germany: O'Reilly Media Inc and dpunkt. verlag GmbH.

Solution Mentors Inc, 2022. *Increase business efficiency with advanced Microsoft Exchange Services.* [Online]
Available at: https://www.solutionmentors.com/platform/microsoft-exchange#:~:text=Exchange%20Online%20market%20share%20reaches,for%20emails%2C%20contacts%20and%20calendars
[Accessed 28 December 2021].

4.2 GLOSSARY

ATTACK SURFACE REDUCTION

Disabling or closing possible vectors of attack inside an IT infrastructure to a necessary minimum including user clients, network components and servers. For example, only open network ports that are necessary (Diogenes, et al., 2016, p. 83).

AWS

Amazon Web Service is the most used cloud service provider that offers a broad range of IaaS, PaaS, and SaaS solutions. It is the main competitor of Microsoft Azure (Davis, 2021, p. 18).

CLOUD

Cloud or cloud computing refers to any digital task that is outsources from an owned computer or server to a provider (e.g., Microsoft Azure, AWS). Large corporations can setup their own private cloud that has the advantages of cloud computing, but the hardware is still owned by the enterprise itself. The main features of cloud computing are distributed systems with agility, on-demand availability, and scalability (Cheshire, 2021, pp. 1,4).

CYBERCRIME

Cybercrime describes every unlawful action that is done by using digital means. It can be subdivided in core cybercrimes including hacking of IT systems or intercepting digital data. Cybercrime in the broader sense includes felonies that do not necessarily require digital means like blackmail or fraud (Pohlmann, 2019, pp. 18-19).

INCIDENT

If an attack on a digital system occurs, it should trigger an incident that is investigated by the IT department weather any damage was done and if further measures have to be undertaken (Engelhart, 2020, p. 69).

IT ADMINISTRATOR

Responsible for maintaining the company´s IT infrastructure. In SMBs often responsible for all IT devices from mobile devices to software and network components (Mayencourt & Peter, 2021, p. 17).

IT SECURITY

Includes three main goals: availability of IT systems, confidentiality of data and the data´s integrity. To achieve those goals technical and processes have to be implemented into a business (Santos, 2021, pp. 69-70).

MICROSOFT AZURE

Microsoft Azure (pronounced: ˈæʒər) is the cloud solution by Microsoft under investigation in this thesis. It offers over 80 different cloud solutions for customers with IaaS, PaaS and SaaS solutions (Microsoft, 2022).

MITIGATION

Mitigation in cyber security means to reduce possible risks that a business threats through policies, technical implementation, or compliance (Santos, 2021, p. 235).

ON-PREMISE

Any digital device, ranging from laptops to servers, that are on the businesses premise or inside their owned data centre. It is mostly used to describe servers and appliance that are company owned and in their data centre (Mather, et al., 2009, p. 7).

REMEDIATION

Remediation comes into play once a attack has occurred and its goal is to limit the attacks damage and actively address the breach. It should not be confused with a post-mortem analysis that is conducted as a forensic action after the incident is dealt with. The remediation is part of the active incident response (Diogenes, et al., 2016, p. 198).

SECURITY SUITE

Suite means a collection of software solutions that work in combination. For example, all Microsoft Azure tools can be referred to as Azure suite (Microsoft, 2022).

THREAT

A threat in cyber security is a possible risk that has not been addressed through technical solutions (e.g. a firewall) or through missing business processes (e.g. phishing workshops for employees) (Mather, et al., 2009, p. 50).

VIRUS

More precise: computer virus. Often used as a collective name that includes any harmful software that poses a threat to any digital system including: trojan horses, worms, ransomware, hijacking or spam ware (Mayencourt & Peter, 2021, pp. 48-49).

VULNERABILITY

A vulnerability in a digital system is a weak spot that could be exploited by an attacker and therefore has to be mitigated through technical measures or risk acceptance (Santos, 2021, p. 11).

4.3 ABBREVIATIONS

Abbreviation	*Meaning*
24/7	all around the clock, every day
AAD	Azure Active Directory
AI	Artificial Intelligence
AWS	Amazon Web Service
Azure	Microsoft cloud service
BSI	ger. Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security) (Germany)
BYOD	Bring your own device
CERT	Computer emergency response team
CIRT	Computer incident response team
CISA	Cybersecurity and Infrastructure Security Agency (USA)
DLP	Data Loss Prevention
DMZ	Demilitarized Zone
EC2	AWS Elastic Compute Cloud
e.g.	lat. exempli gratia (for example)
FBI	Federal Bureau of Investigation (United States)
GDRP	General Data Protection Regulation (European Union)
GPO	Group Policy Object
GPU	Graphical Process Unit
HAW	ger. Hochschule für angewandte Wissenschaften Landshut (University of Applied Science Landshut)
HR	Human Recourses
IaaS	Infrastructure as a Service
IEC	International Electrotechnical Commission
IoT	Internet of Things
IS4IT	Munich based IT service and consulting company
ISO	International Standard Organisation
i.e.	lat. id est (that is)
IT	Information Technology
ITIL	Information Technology Infrastructure Library
IP	Internet Protocol
KQL	Kusto Query Language
KRITIS	ger. Kritische Infrastrukturen (critical infrastructures)
M365	Microsoft 365 (prev. Office 365)
MAC	Media access control (address)
macOS	Apple mac operating system
MFA	Multifactor Authentication
NAS	Network Attached Storage
NCSC	National Cyber Security Centre (UK)

Abbreviation	*Meaning*
NSG	Network Security Group
O365	Office 365 (now Microsoft 365)
OSI model	ISO's Open Systems Interconnection model
PaaS	Platform as a Service
PDF	Portable Document Format
PhD	lat. philosophiae doctor (Doctor of Philosophy)
PHP	PHP Hypertext Preprocessor
RaaS	Ransomware as a service
RDP	Remote Desktop Protocol
S&P500	Standard and Poor's 500 stock market index
S3	AWS Simple Storage Service
SaaS	Software as a Service
SHA	Secure Hash Algorithm
SIEM	Security information and event management
SMB	Small and medium businesses
SME	Small and medium enterprises
SMTP	Simple Mail Transfer Protocol
SOAR	Security Orchestration, Automation and Response
SOC	Security Operating Centre
SQL	Structured Query Language
TPM	Trusted Platform Module
UEBA	User entity behaviour analytics
UK	United Kingdom
URL	Uniform Resource Locator
US[A]	United States of America
USB	Universal Serial Bus
VM	Virtual machine
VPC	Virtual Private Cloud
VPN	Virtual Private Network

4.4 ILLUSTRATIONS

4.5 ATTACHMENTS

Figure 5: Manage Network Security Groups

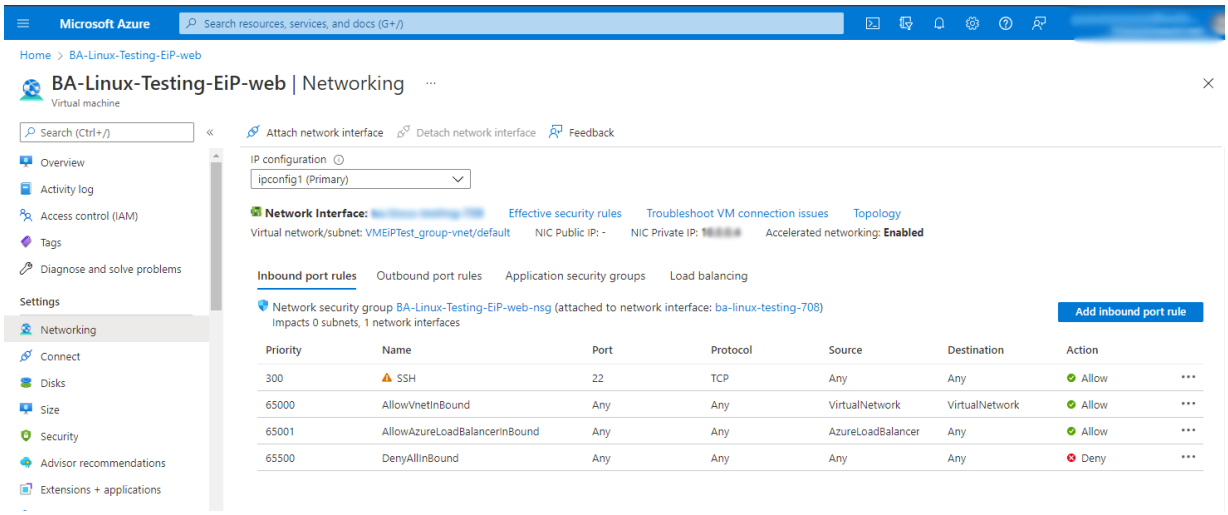


Figure 6: Phishing Attack Simulation dashboard

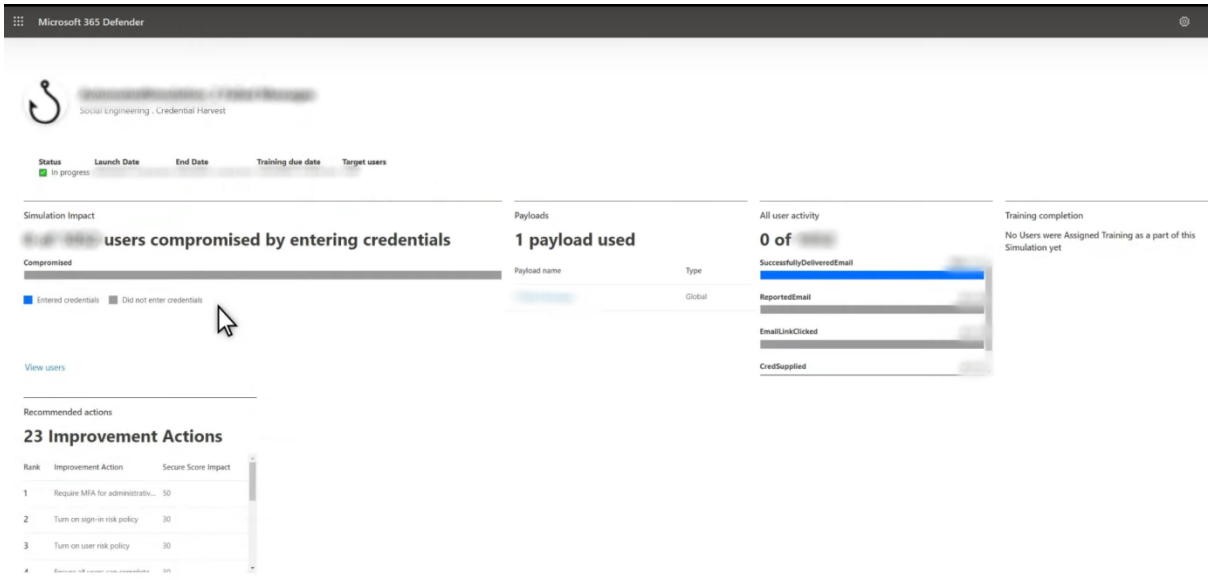


Figure 7:Exchange Online Quarantine dashboard

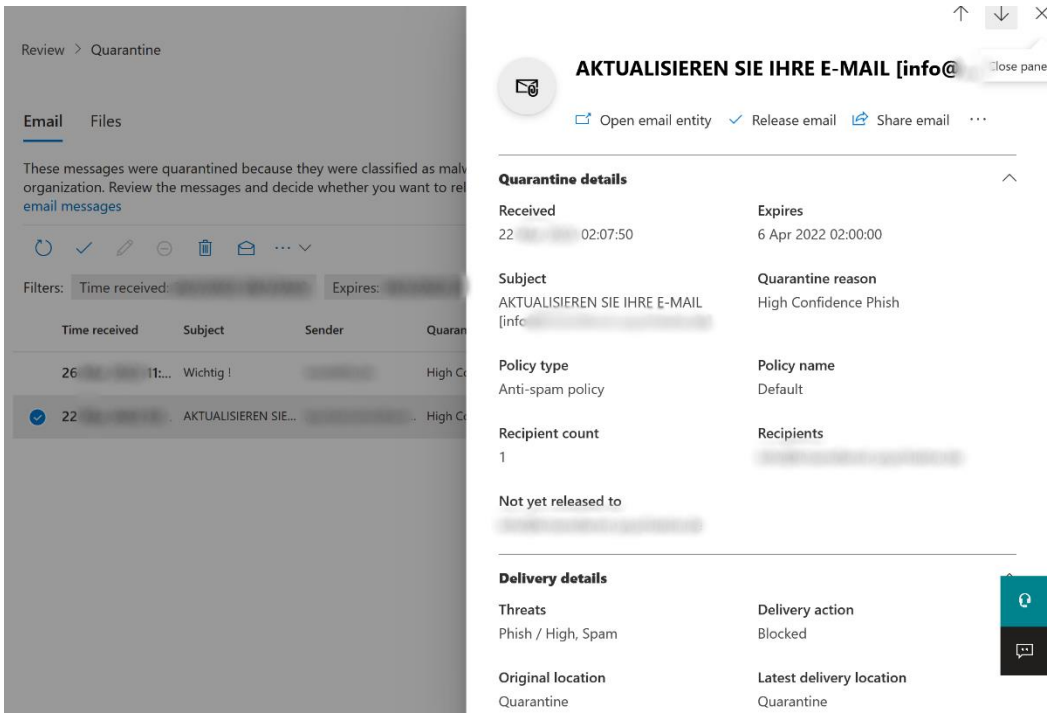


Figure 8: Attack surface reduction in Intune Endpoint Manager

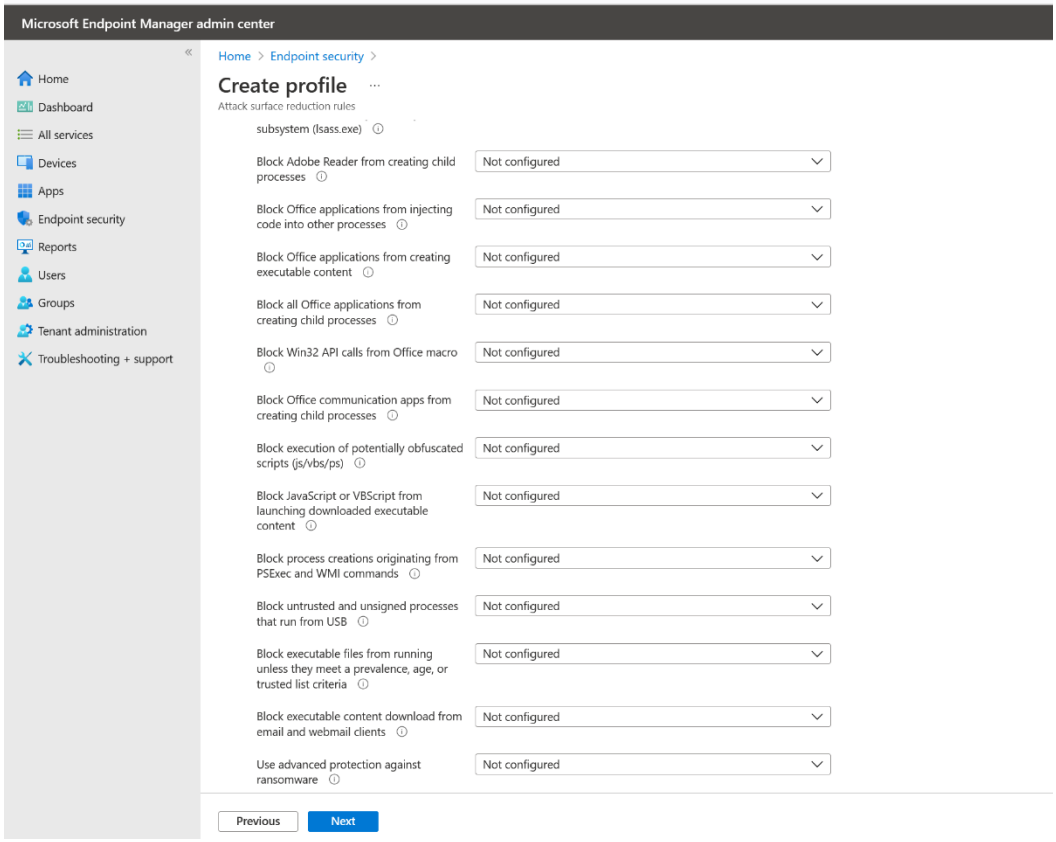


Figure 9: Dashboard Defender

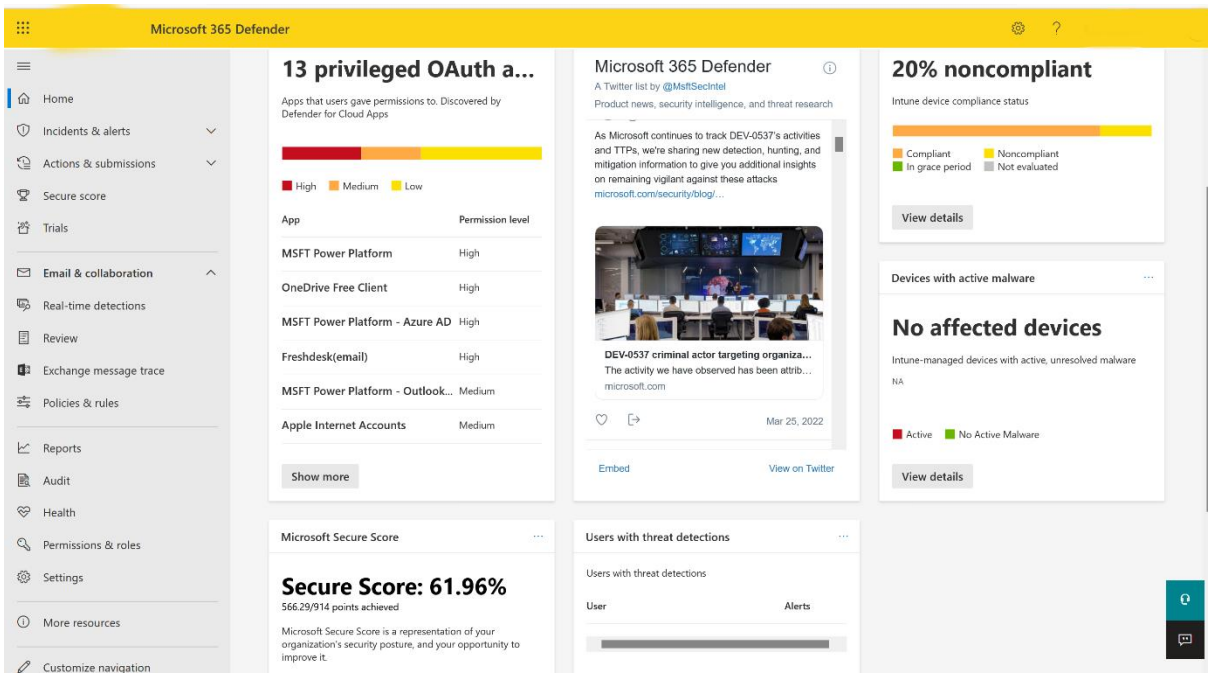
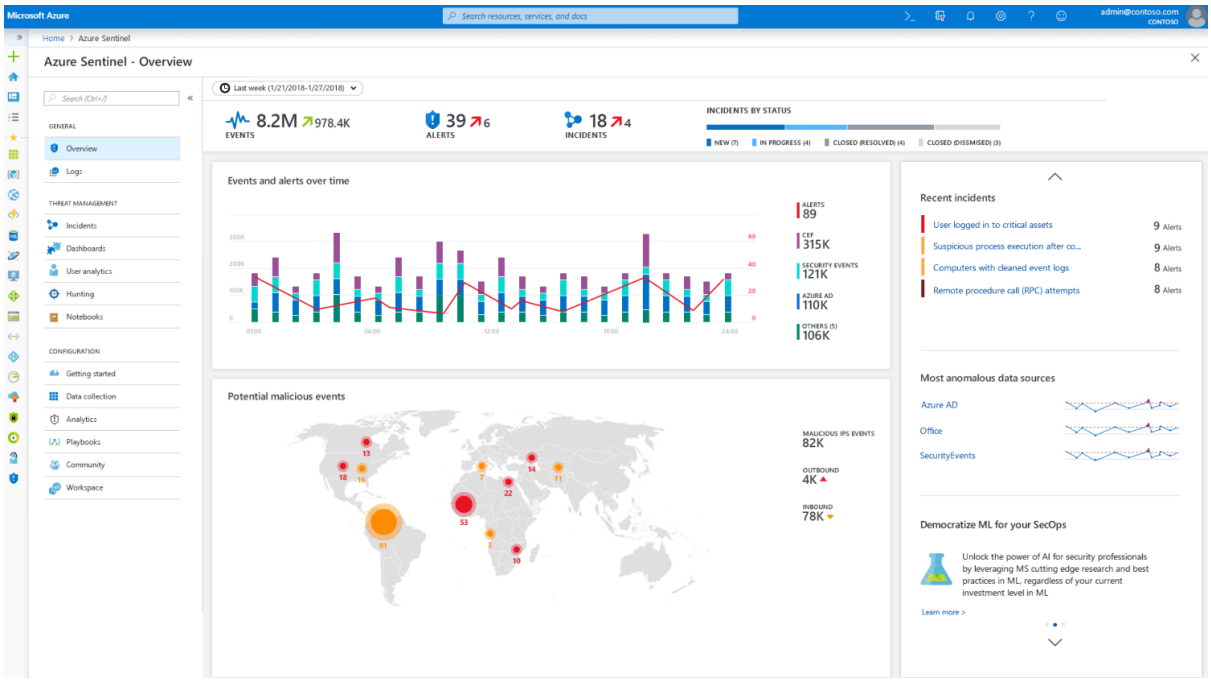


Figure 10: Azure Sentinel dashboard



Source: (Microsoft, 2022) available at: https://azure.microsoft.com/en-us/services/microsoft-sentinel/#overview