CYBERCRIME

A risk analysis for small and medium-sized companies

TABLE OF CONTENTS

EXECUTIVE SUMMARY

WORKING FROM HOME– REMOTE WORK AS A RISK FACTOR

2020 was a great catalyst for digitalization in German resp. companies all over the world: Remote work was expanded, employees were instructed to work from home, and the IT infrastructure became increasingly decentralized. This resulted in three things:

- First, it **destabilized IT landscapes** whose security facilities were only designed for centralized work landscapes.
- Furthermore, **digital communication and collaboration tools** were introduced or expanded—but often without the necessary security measures to quickly provide infrastructure for further work.
- And finally, decentralized working methods **weaken the contact between your employees**. Surprisingly, it has been shown that on-site exchange lowers the probability of falling for a phishing email.

MEDIUM-SIZED BUSINESSES– PHISHING ATTACKS ON VAPS ARE ON THE RISE

Attacks on medium-sized businesses are different from those on large corporations. While VIPs—i.e. upper management—are more likely to be caught in the crossfire of phishing attacks, attacks on medium-sized companies are more widespread.

Employees who are considered Very Attacable Persons (VAP) are targeted. The selection of these particularly vulnerable targets is more promising and leads to the quick success of the attackers in a less complicated way.

This is due to the special structure of (German) small and medium-sized businesses: the company is in one's own hands, one is familiar with one's superiors (up to and including the managing director) as well as one's colleagues. On the one hand, this leads to a climate of trust—unfortunately also in one's own IT security.

CRITICAL INFRASTRUCTURE– OBJECTIVES WITH HIGH SOCIAL RELEVANCE

Despite stricter IT security requirements for critical infrastructure companies, 141 successful cyber attacks were reported by the beginning of November 2020. Of these, 43 were on healthcare providers. In 2019, there were still 121 in the critical infrastructure sector, and in 2018 only 62 successful attempts.* In addition to the healthcare sector, energy, and water suppliers, banks, and insurance companies are also affected. In most cases, such incidents are so-called ransomware attacks that result in a ransom demand for the decryption of data. Due to their criticality, attackers hope to receive quick and high ransom payments to quickly restore operations.

*Source: https://www.faz.net/aktuell/wirtschaft/digitec/mehr-hacker-angriffe-auf-kliniken-und-kritische-infrastruktur-17062421.html

HOW SEVERE IS THE THREAT SITUATION IN GERMANY?

Cybercrime is directed against private individuals and especially against companies, organizations, and institutions.

The greatest danger is posed by identity theft resulting from the disclosure of personal data. This is often achieved through the use of so-called phishing emails. Their damage potential has increased as a result of the Corona crisis: European Union Agency for Cybersecurity (ENISA), for example, reports an increase in phishing emails of more than 600% in the past year.** Cyberattacks that rely on human assistance were and are particularly successful in the Corona crisis.

But why is that? And in particular, how can you successfully protect yourself and your company against such attacks?

*Source: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Lageberichte/Jahreslageberichte/jahreslageberichte_node.html
**Source: https://www.enisa.europa.eu/publications/phishing

THE THREAT SITUATION HAS INTENSIFIED IN 2020

The Corona crisis is causing uncertainty in large parts of the population. For neither privately, professionally nor politically were we prepared for such a situation. And not only that: the new situation suddenly and virtually overnight required new solutions for the continued functioning of our society as well as our working lives. This offered us many opportunities in digitalization but also opened up new attack surfaces for cybercrime.

DIGITIZATION: THE CATALYST FOR CYBERATTACKS

2020 was a great catalyst for digitalization in German companies: Remote work was expanded, employees were instructed to work from home, and the IT infrastructure became increasingly decentralized. This resulted in three things: Firstly, IT landscapes destabilized, whose security measures were only designed for on-site work. Furthermore, digital communication and collaboration tools were introduced or expanded—but often without the necessary security measures to quickly provide infrastructure for further work. And finally, decentralized working methods weaken the contact between your employees. Surprisingly, it has been shown that on-site exchange lowers the probability of falling for a phishing email.

PHISHING & SOCIAL ENGINEERING

Phishing e-mails are fraudulent e-mails that are intended to induce the recipient to perform self-damaging actions. This includes, for example, the direct tapping of passwords and access data or the installation of malware by helping the user. To achieve their goal, the attackers use social engineering techniques. This means the malicious manipulation of people using psychological tricks to cause damage to them or their affiliated companies. This

THE NUMBER OF CYBER ATTACKS IN GERMANY WAS AT A NEW HIGH IN 2020. ACCORDING TO THE BKA, THE NUMBER OF OFFENCES INCREASED BY MORE THAN 15 % YEAR-ON-YEAR TO 100,514.***

***Source: https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2020/Presse2020/200930_pmBLBCybercrime.html

includes, for example, the exploitation of fears, (professional) compulsions, or emergencies.

The motives for such fraud campaigns are manifold, ranging from enrichment through ransomware after data encryption, to long-term damage to (competitor) companies through espionage, sabotage, or stray fire.

THE HUMAN FACTOR IS THE GREATEST RISK FACTOR

As banal as it sounds, interacting with fraudulent phone calls, fake social media requests, malicious emails or websites is THE security hole in your IT system. Successfully compromising your business requires the (active) cooperation of the employee: fraudulent and dangerous malware is reliably detected by modern systems. Therefore, fraudsters now rely on manipulating the component that is not hidden behind technical protection: the human being.

MORE THAN 99% OF ALL ATTACKS REQUIRE HUMAN INTERACTION.*

*Source: https://www.proofpoint.com/de/newsroom/press-releases/human-factor-report-2019-proofpoint-report-zeigt-99-prozent-aller

TYPES OF FRAUD YOU SHOULD BE AWARE OF

PHISHING ("FISHING FOR PASSWORDS")

Fraudulent e-mails serve to enrich the sender by enticing the recipient into self-damaging actions—primarily by tapping into identity features or infiltrating malware/spyware or ransomware to penetrate a (company) network.

VISHING ("VOICE PHISHING") & SMISHING ("SMS PHISHING")

Fraudulent phone calls and SMS are aimed at grabbing important account data and identification features. Vishing in particular is also often used to obtain information on important decision-makers. A cyberattack is carried out afterward with the information obtained.

SPEAR PHISHING & WHALING

A special form of phishing that very specifically targets people in upper management or critical information in the company (finances, patents, trade secrets).

(CALL) ID SPOOFING

A hacker forges the identity of a person or authority to make supposedly legitimate calls or write e-mails. In this way, deceptively genuine (but faked) mail accounts are created, real mail accounts are taken over by malware or the display of telephone systems is manipulated remotely. ID spoofing is primarily aimed at gaining information for further criminal activities.

BUSINESS EMAIL COMPROMISE (BEC)/ CEO FRAUD/ IDENTITY THEFT

A major, but still underestimated risk for companies is the so-called CEO Fraud. In this case, fraudsters fake the identity of the CEO (or other important managers) to put pressure on employees. For example, they are asked to make a quick payment or to pass on secret internal information. The required information is often available online (imprint, press releases, or social media) or has been obtained through vishing/phishing campaigns.

Unfortunately, such scams are getting better and better and can no longer necessarily be recognized as such at first glance, even by trained users. The unknown, rich relative from the most absurd parts of the world has meanwhile been replaced by deceptively genuine-looking PayPal e-mails, for example, which specifically want to "fish" for users' passwords and credit card data.

Poor grammar and incorrect vocabulary are also rarely found in modern, well-crafted malware spam. According to the BSI*, even an HTTPS link is no longer a guarantee of security—HTTPS links are already used in around 60% of registered malware spam in 2019/20. Although the security certificate is supposed to identify secure homepages, it can be licensed free of charge on the internet. Regardless of whether the content is safe for the consumer.

THE BIGGEST THREAT TO SMES COMES FROM IDENTITY THEFT & MALWARE (RANSOMWARE/ SPYWARE), WHICH ALMOST ALWAYS INVOLVES HUMAN INTERACTION.

*Source: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf

MODERN (MALWARE) SPAM EXPLOITS OUR WEAKNESSES

These are usually emotional reasons such as performance and time pressure. Or human routines such as tiredness and thus carelessness in the morning. Often, a direct connection to the recipient and thus high relevance is feigned. Or heuristics and automatisms of the persons are exploited (kundensupport@arnazon.de). Professional constraints in combination with emotional activation also ensure a high click rate (e.g. a dissatisfied "customer").

96% OF GERMAN COMPANIES HAVE SUFFERED A BUSINESS-DAMAGING CYBER ATTACK IN 2019/20.*

*Source: https://industrie.de/it-sicherheit/96-prozent-deutscher-unternehmen-haben-mindestens-einen-cyberangriff-erlitten/

THE PSYCHOLOGY BEHIND SOCIAL ENGINEERING

PRESSURE & FEAR

HELPFULNESS

AUTHORITY

CURIOSITY

PRAISE & FLATTERY

NEED FOR INFORMATION

TRUST & INTIMACY

EXPLOITATION & MANIPULATION

TARGETING THE SME SECTOR

ATTACKING VAPS INSTEAD OF VIPS

Attacks on SMEs are different from those on large corporations. While the VIPs—i.e. the upper management—are more likely to be caught in the crossfire of phishing attacks, attacks on medium-sized companies are more widely spread.

Employees who are considered very attackable persons are targeted: These are mostly new employees, but also finance departments or still inexperienced admins with extended rights.

The high success rate of such attacks is due to the special structure of the (German) SME sector: the company is owned by itself, people are familiar with their superiors (up to the managing director) as well as their colleagues. On the one hand, this leads to a climate of trust—unfortunately also in one's own IT security

On the other hand, attackers promise themselves a higher and faster need to settle a ransom payment. On the one hand, this is due to the lower liquidity of smaller companies, for which and their owners a standstill can threaten their existence, and on the other hand, it is also due to the shorter decision-making paths with simpler hierarchical structures.

UNEXPLAINED EMPLOYEES

The fact that medium-sized companies have a higher number of VAPs than large companies is also due to a lack of employee education. Due to their size (and thus the supposedly small attack surface), SMEs lull themselves into a false sense of security. And they save on employee training on phishing and social engineering, for example.

WEAK IT SECURITY INFRASTRUCTURE

Lower expenditure on internal IT also means a smaller budget for necessary security measures such as backups, higher security levels, and emergency plans for defense and damage limitation in the event of cyberattacks. Often, the most important basic protection in the form of multifactor authentication is already missing.

SMES IN THE FOCUS OF CYBERCRIME

"We are too small—it's not worth it at all", this fallacy of many SMEs often becomes very expensive. As the BKA has already seen an acute increase in cyber attacks on small and medium-sized enterprises for years. Especially in the crisis year, attacks have increased, and the quality of these has also changed.

This also has something to do with the fact that the place where we work has changed. The remote setup in the workspaces at home has made new vulnerabilities in the IT infrastructure visible, such as the inadequate protection of private networks. Moreover, due to the physical separation of employees, attacks are only noticed or reported lat—if at all. This applies not only to reporting to IT but also to the daily exchange before possible new threats.

And phishing emails are still the gateway for criminal activities. Nevertheless, it would fall short to ignore technical barriers and rely only on employee training. We will show you why in the following.

*Source: https://www.bitkom.org/sites/default/files/file/import/181008 Bitkom Studie Wirtschaftsschutz 2018 NEU.pdf

ARE STAFF TRAININGS ENOUGH?

Unfortunately, no! Because all it takes is one employee opening a link or attachment to break into your system.

Nevertheless, the targeted training of your employees is a first step towards preventing such attacks. For example, on the topics of phishing/social engineering to sensitize them to these issues. At the same time, improved backup structures with more frequent and so-called offline back-ups (i.e. back-ups that cannot be changed from the network) are part of a precautionary plan against cyber, especially ransomware attacks. However, you must bear in mind that the possible publication of stolen data will result in GDPR lawsuits.

ORGANIZATIONAL MEASURES & PROCESSES

The basis for the successful implementation of all non-technical measures against phishing attacks is to design your company processes in such a way that identity misuse can be virtually ruled out. This includes, for example, a 4-eyes principle for financial transactions or limited access management to critical systems.

In addition, you must establish clear communication rules. This includes central and comprehensive rules on the use of e-mails, intranet, or other internal and external communication and collaboration tools. On the other hand, there is the question of to whom a phishing suspicion should be reported. The establishment of a positive security culture is crucial so that employees report suspicious activities and their own mistakes proactively and without fear.

CRITICALLY EXAMINE ONLINE PRESENCES

Today, companies and their employees are necessarily present on many platforms. Nevertheless, you should question which information about your company and your employees is freely available—and which of this information should better not be.

Actively deal with your online and social media presence and develop a code of conduct as well as guidelines for the social media presence of your company and its employees.

TRAIN EMPLOYEES

Employees are your capital—also when it comes to your IT security. Because without interaction with people, today's cyberattacks can hardly get into your system, because—with the necessary care—the systems can intelligently recognize malware.

Therefore, you should not save at the wrong end and invest in (simulation) training on the topics of phishing and social media. There are various approaches to this, which you can carry out internally or with external service providers. These include simulations and dry runs of internal phishing attacks, concepts for initial training of new employees and ongoing measures for all colleagues, seminars, webinars, web-based training, and e-learning tools. However, repeated re-sensitization should take place here, which is why clearly defined, smaller and repetitive units make more sense than large-scale and complicated initiatives.

CONSEQUENCES OF PHISHING FOR YOUR COMPANY

FAILURE OF THE COMPLETE OPERATION

FINANCIAL LOSS/ WIRE FRAUD

DATA LOSS/ DATAENCRYPTION

PUBLICATION OF CONFIDENTIAL DATA

GDPR-VIOLATIONS AFTER DATA THEFTS

LOSS OF REPUTATION

Cause: compromise of access data/ accounts

SOCIAL ENGINEERING

RANSOMWARE-INFECTION

OTHER MALWARE-INFECTIONS

TECHNICAL BARRIERS

PROTECT EVEN IF THE HUMAN BEING FAILS

JUST ONE EXAMPLE*

October 2020: Hackers were able to phish off data on employee accounts at Swiss universities as part of a phishing campaign. They used the information thus obtained to make targeted changes to recipient accounts for salary payments in the HR system/HR master data in the system. A six-figure loss was incurred.

Establishing an effective, technical hurdle in the form of multifactor authentication for changing important master data could have compensated for human error.

*Source: https://www.it-daily.net/shortnews/25650-hacker-stehlen-sechsstellige-summe-von-schweizer-hochschulen

TECHNICAL BARRIERS ARE THE BE-ALL AND END-ALL FOR SECURE CORPORATE IT

Security software is constantly evolving: today's anti-virus and anti-malware programs usually function proactively, i.e. their underlying algorithms can identify even new, as yet unknown malware based on certain heuristics. And block or delete it before it can do any damage.

ESTABLISH BASIC TECHNICAL SECURITY MEASURES

Regular and timely updates of all operating systems, server and application software increase the basic security of your systems. This is because there is hardly any software on the market that does not come with bugs or security holes in the code. Old and known bugs are a popular target for attackers; the only way to combat them is to install the patches provided by the manufacturer.

Newer, often still unknown bugs, on the other hand, are usually not (yet) a worthwhile target: the search for the latest, novel vulnerabilities (in a race against the manufacturers) is very costly and not lucrative enough in itself, to begin with. For this reason, attackers are focusing less on internal, technical vulnerabilities and more on an external vulnerability that is easy to outsmart—the user in front of the PC.

THE HUMAN VULNERABILITY

Before getting to this, there is another technical weak point that must be skillfully overcome: the automated malware scanner of our e-mail inboxes: if a fake link is hidden here that leads to a website containing malware, or prompts employees to enter their data there, the scanner (logically) cannot detect it.

It is precisely this technical gap that attackers use to get to their target: They rely on the system not recognizing that the content behind it is harmful to the user.

A cleverly prepared and coherently formulated phishing mail often enough leads—despite supposed clarification—to an employee following the instructions and opening a link or an attachment: And thus unwittingly builds a bridge for the attackers by taking actions there that outsmart your security systems.

Once attackers have an employee's password, they can easily use it to access that user account—and the company's data, systems, and network.

VPN CLIENTS, ANTIVIRUS/ ANTIMALWARE, AND FIREWALLS ARE NOT ENOUGH

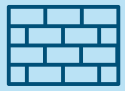
Endpoint protection such as client firewalls, malware protection, or VPN clients is mandatory for a secure IT environment that includes remote workstations. Regular (offline) backups also safeguard you for worst-case scenarios. This means you are quickly up and running should other security measures not have taken effect. Encrypted data transfer also ensures that hackers cannot siphon off relevant data and information. Nevertheless, none of these measures secures your weak point—your employee.

SECURE YOUR USER ACCOUNTS FROM IDENTITY THEFT WITH IAM & MFA

Your technical barriers shouldn't end with firewalls, VPN clients, and anti-virus software. Effective technical barriers are based in particular on sensible identity and access rights management as well as mandatory multifactor authentication for all employees. This is the only way to secure identities and protect them from misuse.

In addition, the reduction of externally accessible systems to a minimum as well as a proper internal segmentation of the networks form a further security level. To prevent deeper infection of your systems, you should also introduce an increased requirement for password security with multifactor authentication (MFA) on specific machines, systems, or areas. Most especially for administrators and those with remote access privileges.

SOFTWARE UPDATES



FIREWALL

ANTI-VIRUS/ ANTI-MALWARE

IDENTITY & ACCESS MANAGEMENT

MULTIFACTOR AUTHENTICATION

EXCURSUS: CRITICAL INFRASTRUCTURE COMPANIES

Special medium-sized companies are the critical infrastructure companies. The functioning of our society depends very centrally on the supply by these. Whether it is our energy supply or our health care—a failure of the infrastructure has consequences in all areas of life.

It is therefore essential to provide special protection for these facilities. In addition to prevention and emergency plans at the physical state of the facilities, this increasingly includes the question of the security of the controlling IT systems.

The underlying IT has become increasingly complex and multi-layered in the course of digitalization: The advent of the (I)IoT (Industrial Internet of Things) has deeply networked plants and machines. Even the selective failure of a cog in the system can therefore have unforeseen, protracted consequences.

As a result, a successful attack has an immensely higher potential for damage, as the consequences extend beyond the company to society. As a result, (IT) security requirements are stricter than for other companies. At the same time, securing the IT systems of critical infrastructure operators is not an easy undertaking. On the one hand, these are private-sector companies of various sizes. For another, the IT structures used to have a long life cycle, which is why they often do not have the necessary security updates or do not have them promptly.

Despite stricter requirements, 141 successful cyberattacks were reported by early November 2020. Of those, 43 were on healthcare providers. In 2019, there were still 121 in the critical infrastructure sector and only 62 successful attempts in 2018.* In addition to healthcare, energy, and water suppliers, banks and insurance companies are also affected. In most cases, such incidents are so-called ransomware attacks, which entail a ransom demand to decrypt data. Due to their criticality, attackers hope to receive fast and high ransom payments to quickly resume operations.

*Source: https://www.faz.net/aktuell/wirtschaft/digitec/mehr-hacker-angriffe-auf-kliniken-und-kritische-infrastruktur-17062421.html

DOUBLECLUE – THE SOLUTION FOR YOUR BUSINESS

DoubleClue protects your corporate network from unauthorized and malicious third-party access. The software combines state-of-the-art Identity & Access Management (IAM) with state-of-the-art Multifactor Authentication (MFA) and has additional security features that make your employees' daily work easier.

IDENTITY & ACCESS MANAGEMENT

The easily structured IAM platform allows you to centrally manage accounts, identities, and accesses. At its core is access management to systems and applications with automated authorization management and adaptive access policies for applications and user groups. This also allows the establishment of a so-called Privileged Access Management (PAM).

TWO-FACTOR AUTHENTICATION

Easy-to-implement two-factor authentication prevents intrusions on and into your network. DoubleClue offers you all the possibilities of a modern, password-free login: Choose the variant that suits you best from a variety of authentication options.

SINGLE SIGN-ON (SSO)

Your employees work simultaneously in different applications for which they need separate accounts with their access data. Thanks to Single Sign-On, a single login to the DoubleClue UserPortal is all it takes to gain access to all the applications they need - with just one click.

PASSWORDSAFE WITH AUTOFILL FUNCTION

DoubleClue PasswordSafe greatly simplifies the management of many, even complex, passwords. Easily store your passwords in one place and access them in bundles—directly from the web application or mobile app. MFA and encryption ensure that passwords are kept safe in your safe. Autofill lets you conveniently log in anywhere from the DoubleClue app.

DOUBLECLUE KEEPASS PLUGIN

The globally popular open-source password manager KeePass lacks two things by default for use in an enterprise environment: multifactor authentication and the ability to share passwords with colleagues, partners, and service providers. The DoubleClue KeePass plugin allows easy import and export of password (kdbx) files between the two systems.

DOUBLECLUE APP FOR iOS & ANDROID

Users today expect high usability. Therefore, DoubleClue offers you the possibility to manage passwords and approvals via a modern and clear app on your mobile device.

DOUBLECLUE CLOUDSAFE

Important and confidential documents should never be sent via unencrypted emails. DoubleClue CloudSafe therefore not only allows you to centrally store sensitive data in an MFA-protected, inaccessible area within your own IT infrastructure. It also opens up the possibility to securely share this access with your employees, partners, or service providers—without your data leaving the server.

To the product data sheet

DOUBLECLUE–USE CASES

PROTECTION OF REMOTE WORK

2020 has been a catalyst for digitization for collaboration in distributed teams. This includes the creation of remote workstations in an insecure workspace environment while working from home, as well as the new introduction and expansion of digital communication and collaboration tools (in the cloud/ hybrid).

DoubleClue secures your employees' log-ins and all applications with multifactor authentication. You can centrally control all access rights via the clear IAM tool.

The integrated PasswordSafe for centralized password management and single sign-on to all applications also increases employee productivity with great usability.
In the CloudSafe, you store documents securely in a central location. You can share access to them with internal and external stakeholders, so not only are your employee identities secure but so are your corporate secrets.

SECURING CRITICAL INFRASTRUCTURE

Critical infrastructure companies need deep protection of their systems from unauthorized access by third parties. In addition to the healthcare industry, this is especially true in the energy sector.

HEALTHCARE INDUSTRY

Cyberattacks in the healthcare industry have increased sharply in the past year. At the same time, digitization is advancing rapidly to simplify processes for diagnoses and treatments. However, a hack or data leak at this point would be fatal.

The healthcare industry also has special IT security requirements. Medical devices are often connected to the network in addition to office computers and printers. Separate clients can be used to separate different areas and define different access rights. Servers that store confidential patient data, for example, can be secured so that only individuals with special access requirements can access them.

For this purpose, you can create user groups with different criticality ratings in DoubleClue. Using a so-called PAM (Privileged Access Management), particularly strict individual access and authentication solutions can be applied to especially critical systems.

In addition to the reliable protection of (subdivided) networks in medical practices, pharmacies or hospitals, we have also developed solutions for so-called shared access to individual machines, which exclude misuse and still do not interrupt the work processes of your employees.

ENERGY SUPPLIERS

Here, the focus is particularly on control networks in the areas of water, electricity, and gas supply. Like the healthcare industry, utilities require critical access rights and strong authentication solutions. Here, too, we rely on the subdivision of user groups using PAM.

HWS GRUPPE

HWS INFORMATIONSSYSTEME GMBH

The HWS Group offers its customers comprehensive IT services, software development, and consulting, especially in the areas of IT infrastructure, cloud operations, and identity protection. More than 150 employees from Neustadt an der Aisch (Middle Franconia) and the nearshore delivery center in Malta support both DAX corporations and upper mid-sized companies in holistic IT projects. Thanks to a progressive and demanding service approach, we have been convincing customers as a reliable and close partner for more than 20 years.

IT Security made in Germany!

Our comprehensive IT security solution "DoubleClue" provides companies worldwide with secure identity and access management as well as a strong multifactor authentication solution.

Learn more about us and our services and software products at
hws-gruppe.de & **doubleclue.com**.

HWS INFORMATIONSSYSTEME GMBH
Wilhelmstr. 16 | 91413 Neustadt a. d. Aisch
+49 (0)9161 6239 200 | requests@doubleclue.com

DOUBLE CLUE
CLEVERLY SECURES IDENTITIES

We are Partners

Allianz für Cyber-Sicherheit
Partner