CRASHTEST **SECURITY**

IT SECURITY

FOR MEDIUM-SIZED BUSINESS

FOR MEDIUM-SIZED BUSINESS
IT SECURITY

DIGITIZATION

Digitization is the most important and probably most discussed topic for companies today. Medium-sized companies, in particular, are increasingly trying to set themselves apart from the competition with outstanding digital solutions. However, the high digital potential does not come without a certain risk.
The more digital presence a company has, the greater the potential attack surface for hackers and cybercriminals. As a result, many small and medium-sized enterprises (SMEs) wonder why they are the target of a hacker attack. Even though large companies have larger volumes of data, hackers are increasingly targeting SMBs.
In the „State of Cyber Security in Small & Medium-Sized Businesses“ report by the Ponemon Institute, 66% of the companies attacked in 2019 were SMEs.[1]

WHY ARE MID-SIZED COMPANIES BEING TACKLED EVEN THOUGH LARGE COMPANIES HAVE MORE DATA?

It is generally easier to hack small and medium-sized companies, as they usually do not (yet) have sufficient security standards and rules in place. In addition, most companies lack the budget or personnel to provide the necessary level of security, and IT security is not a top priority[2].

In addition, SMEs often have interesting data that can be a target for hackers. For example, it is usually intellectual property, significant innovations, or sophisticated technology that people outside the company could be after.

1 Keeper Security
2 Information Age

TABLE OF CONTENTS

However, the biggest concern for businesses - according to the Ponemon Report - is that customer data can fall into the wrong hands[3]. Small or medium-sized businesses tend to be on a tight budget, and time is an even more precious resource. Therefore, significant investments in IT security can be beneficial, but there are also basic things that companies can do for their security that cost little or no money.

In the following, we would like to show you some basics which should be included in the safety concept of every company. These basics can then be considered, for example, in a TARGET-ACT analysis, whereby the current state of security is evaluated and, based on this, a TARGET state is defined, which is to be achieved in 6 months.

3 CISION PR Newswire

1. MAKE IT SECURITY YOUR PRIORITY

Every company should consider IT security as a foundation for the survival of the business[1]. Therefore, it is particularly worrying that this issue is still not prioritized in almost half of SMBs. As Amazon's VP & CTO said at the Bits & Pretzels conference „Without Security, you have no business!". This statement from a leading CTO supports the argument that insufficient security can put a company's customers, and therefore its entire business, at risk. Accordingly, IT security should have the same priority in both development and management as, for example, software functionality or customer service. If the developed functions contain security gaps, the company will lose customers and may even have to file for insolvency.

1.1 SECURITY STARTS FROM THE TOP

When IT security is on the management's agenda, it ensures that the problem is anchored at the highest level in the company and is a high priority. The current security status should be discussed in weekly meetings and access to all departments at all times. As with any critical issue, proper management is essential to keep IT security in employees' minds at every decision.

1 INC.

„WITHOUT SECURITY YOU HAVE NO BUSINESS!"
- Werner Vogels
(VP & CTO Amazon)

1.2 CREATE AND ALLOCATE RESOURCES

No company has endless resources available for a particular area. But in any case, the resources should be created to secure the company. Fixing a security vulnerability after it is found is ten times more expensive than securing it in advance. That's why it's crucial to create the budget, personnel, and IT infrastructure to maintain the integrity of the enterprise. However, companies that do not have the financial resources for full-time security experts should make at least one person responsible for IT security (e.g., the CIO or CTO). This way, every decision is double-checked to see how it impacts the security posture.

1.3 MATCHING THE PRIORITIES OF THE DIVISIONS

IT security should be a priority, but this does not mean that a company should devote all available resources. SMEs, in particular, should find sub-priorities and prioritize securing essential parts of the business. Not every company has the same data structure or the same systems. Therefore, this is not to be understood as a checklist but rather as a possible guideline on how a basic level of security can be created, which companies can then build individually. A „threat analysis" can be helpful here, revealing which vulnerabilities should be treated with which priority. The main headings of this white paper can be used as starting points.

2. EMPLOYEES ARE THE FOUNDATION

According to surveys, untrained employees are the main reason for security incidents in SMEs. Although this could be easily prevented, many SMEs still place too little emphasis on raising their employees‘ awareness of IT security issues. Especially for companies with valuable information and data, all employees must have sufficient knowledge regarding IT security[1].

2.1 A PART OF THE CORPORATE CULTURE

Addressing the issue at the highest level in the company is essential but not sufficient if most employees are not aware in their daily work of the consequences that incorrect behavior can have for the company‘s security.
To ensure security is integrated into the culture, a security plan can outline what actions each employee can take to prevent hacking attacks.
Such an approach is critical if you plan to have your company ISO 27001 certified.

Every employee should know basic measures through the plan and apply them in their daily work.

Part of such a plan can be, for example, password rules that every user of the system must follow. We will show more examples in the next chapter.

In addition, the company’s security status can be shown regularly in meetings using a dashboard to see the impact of their work on the company’s security. By increasing awareness, you can ensure that the protection of the company‘s data is present in the mind of each employee.

54% **EMPLOYEES CAUSE 54 PERCENT OF ALL SECURITY BREACHES.**

2.2 IT SECURITY COACHING FOR EMPLOYEES

All beginnings are challenging, but the little things are enough. For example, they are telling employees to lock their PCs when they leave the workplace. It is easy to obtain internal company data if there is no encryption or protection. Another simple measure is to perform software updates whenever possible. Hackers use known vulnerabilities to get into systems. Updates usually include bug fixes and security enhancements that make life much harder for hackers.

For more specialized topics (e.g., phishing attacks), advanced training workshops are recommended. This allows employees to identify and report attacks early. A reward system for reporting vulnerabilities or attacks can be successful in motivating employees to address these issues. Special training courses on secure programming should be offered for employees who work directly on the IT infrastructure, especially software developers.

1 New York Times

3. INTRODUCTION OF A PASSWORD CULTURE

As mentioned earlier, rules about passwords should be integrated into every company‘s security plan. These rules should be applied not only by employees but by all users who have access to the system. There are a few things to keep in mind when passwords are created.

3.1 PASSWORDS MUST BE STRONG ENOUGH

Hackers have databases of passwords that are often used, so the security level increases significantly with the strength of a password. Experts recommend passwords that consist of at least 20 characters and contain special symbols so that hackers cannot easily crack them.

3.2 SPECIFIC PASSWORDS FOR EACH APPLICATION

However, if a password is found out, hackers should not have immediate access to every user application. Therefore, to secure the entire IT infrastructure, specific passwords must be used for each application.

3.3 PASSWORDS SHOULD BE CHANGED OFTEN

It is recommended that system users change their passwords every 30 to 60 days. A strong password with more than 20 characters will take hackers more than 60 days to decrypt. In addition, by changing passwords regularly, hackers have to start from scratch, and applications become more secure.

3.4 PASSWORD MANAGER AS AN AUXILIARY TOOL

Strong and specific passwords are difficult to remember, and writing them down is not recommended. Password managers help to keep track of passwords, and users only need to remember one master password. However, this should then be strong enough to protect all others adequately.

3.5 TWO-FACTOR AUTHENTICATION FOR ADDITIONAL SECURITY

Two-factor authentication is an effective measure to provide an extra layer of security. Even if a hacker solves a user‘s password, the account must be unlocked, e.g., by an SMS code. However, this then requires a second device to be connected to the user‘s account.
As you can see, there are several simple and inexpensive measures that every employee can take through password protection alone to secure the company‘s IT landscape.

4. ACCESS CONTROL FOR ALL USERS

The more users a system has, the more potential attack targets and vulnerabilities the system has through these users. Therefore, it is imperative to control which user has access to the system.

4.1 INTRODUCTION OF USER VERIFICATION

The first step in securing data is to control who has access to it. Especially users from outside the company should be verified and monitored. Any input can be bad for security, and sufficient verification should be implemented for each user. The password basics described in Chapter 3 should therefore apply to every user in the system.

4.2 ONLY THE MOST NECESSARY RIGHTS FOR ALL USERS

After verifying each user, it is vital to be as restrictive as possible with their rights. Officially, this measure is called the „Principle of Least Privilege.” Users should be given as few rights („Least Privileges“) as possible at the beginning. Later, of course, main users and administrators can be given additional privileges. The division of responsibilities is another

critical basis. In its report, the SANS Institute suggests that users should be divided into different roles.

Even top managers should only be able to see what they need for their work. This keeps corporate data as secure as possible and allows employees to focus on what they are working on. The number of these primary users should be kept as low as possible. Even these users should be permanently monitored and - as a role model for other users - comply in particular with the IT security rules.

5. DATA SECURE THE BUSINESS

After the people who use it, data is a company's most valuable asset. You need data to know and understand your customers. Customers, therefore, want their data to be safe with you. Cloud services, e-commerce companies, or organizations working with mobile applications are especially vulnerable to data breaches and manipulations.

At the latest since the introduction of the General Data Protection Regulation (GDPR) in May 2018, data protection is a vital topic for all companies in the European Union, as neglect can lead to high fines and liability risks[1]. Additionally, other countries in North America and APAC have similar regulatory legislation concerning data privacy.

5.1 DATA RISKS IN COMPANIES

There are some risks to SMBs that have important business and customer data. Kunden vertrauen Unternehmen genug, dass Customers trust companies enough to provide them with their data. Therefore, this trust should not be destroyed and the data should be secured at all times.

Furthermore, there is an integrity risk in that enterprise systems must be continuously secured against unauthorized modification. Finally, there is the risk of data availability, as this data is necessary for operational business. Losing access to this data can result in large financial losses.

5.2 DATA BACK-UPS

Ransomware attacks are becoming more common, and 58% of respondents in the Ponemon Institute survey said these attacks had severe financial consequences for their business. Ransomware attacks are attacks in which hackers block access to data for the user. The user can only access the data (or, in the worst case, the entire system) after decryption, for which the hackers often demand a ransom. Data backups can ensure that you have access to your data even in the event of such an attack.

5.3 CYBER VAULTS

Ideally, organizations have a Cyber Vault separated from the production and backup systems via „Air Gap." This „Air Gap" is only closed when data is copied. Such a cyber vault contains the organization's essential data needed for minimal operations. For example, after the Sony Pictures hack, the company had to pay employees by paper checks because even simple systems were no longer available[2].

1 General Data Protection Regulation

2 Business Insider

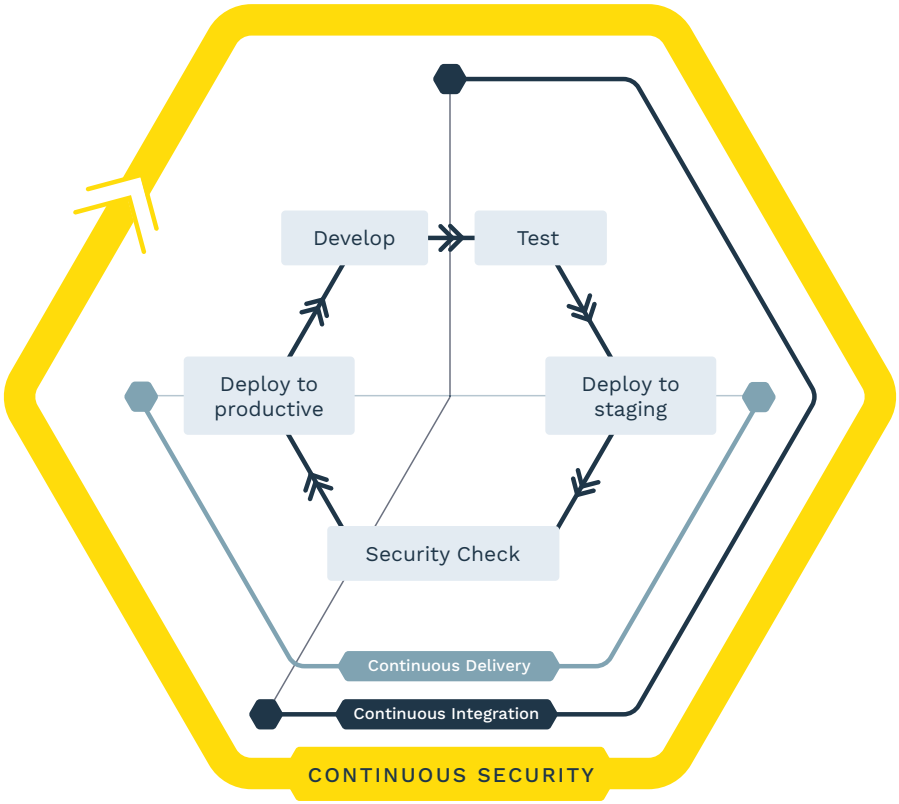
6. CONTINUOUS SECURITY TESTING

All of the above measures can be easily integrated into companies to minimize the risk of vulnerabilities. However, it is clear that people always make mistakes, and even the developers‘ code can never guarantee complete security. One way to ensure that the company is permanently protected is „continuous security testing.” Manual penetration tests are too expensive and time-consuming in agile software development, which uses continuous integration and deployments (see Fig. 1). In these forms of agile development, applications are developed and released in short cycles. Only automated tests can be used to test each version in this process, as manual tests for each new development stage would represent considerable time and financial effort. Existing vulnerabilities are found before a new software version is released. The latest version is released on time.

Applications such as the Crashtest Security Suite offer automated solutions that can be integrated into the development process from the very beginning.

Continuous vulnerability testing allows developers to fix these problems directly. This gives them more time to develop the features that add real value to customers and create a competitive advantage for your business. In addition, by providing direct feedback on the current security posture of your web application and an integrated knowledge base, developers are helped to integrate secure programming into their daily workflow. Since most mid-sized companies do not have a high level of IT security expertise, this additional information can help in any business area.

In addition, managers receive direct information about the company‘s security status through integrated dashboards and email reports after each application scan(s).



7. THE CONCLUSION

As described at the beginning, this WhitePaper contains essential basics on IT security in SMEs. Below we have summarized the most critical points once again.

- Web applications are always vulnerable to hacker attacks and always will be. How these vulnerabilities are addressed and avoided depends on management, developers, and each employee.
- Securing a business is not as complicated as it seems, especially SMBs can use some simple and, most importantly, inexpensive basics.
- Employees are the foundation of any company's IT security. Therefore they should be supported and trained permanently.
- If there is a security culture in the company, it is more likely that vulnerabilities can be identified and fixed quickly.
- Automated security tests help companies have a permanent overview of IT security and be able to act at any time.

ABOUT CRASHTEST SECURITY

Crashtest Security is a Munich-based IT security company.

As an innovator of cyber security solutions for web applications, it develops automated solutions for vulnerability analysis.

Based on artificial intelligence, vulnerabilities are detected, protection against hacker attacks is increased and transparency for companies, users and developers is created.

Visit our website for more:

WWW.CRASHTEST-SECURITY.COM

CRASHTEST SECURITY GMBH

Leopoldstraße 21
80802 Munich
+49 (0)89 215 41 665

info@crashtest-security.com

SOURCES

https://www.keeper.io/hubfs/PDF/2019%20Keeper%20Report%20V7.pdf

https://www.information-age.com/cyber-security-still-not-top-boardroom-priority-123468999/

https://www.prnewswire.com/news-releases/ponemon-cyberattacks-on-smbs-rising-globally-becoming-more-targeted-and-sophisticated-300933394.html

https://www.inc.com/oracle/cyber-security-survival-tips-for-smbs.html?cid=search

https://gdpr-info.eu/issues/fines-penalties/

https://www.nytimes.com/2016/01/14/business/smallbusiness/no-business-too-small-to-be-hacked.html

https://www.businessinsider.com/sony-hack-caused-the-company-to-use-old-technology-2015-6?IR=T

https://www.sans.org/white-papers/35792/