CRASHTEST **SECURITY**

RESEARCH PAPER

THE WEBSITE AS A TARGET

HOW SECURE ARE THE WEB PRESENCES OF THE GERMAN INDUSTRY?

THE WEBSITE AS A TARGET

Crashtest Security, the leading German provider of web application security, set itself the goal of increasing cyber security in Germany and making companies more resilient to attacks from the web. For this goal, they needed a measurement basis and decided to use the online presences of 5,353 companies listed in German industry associations.

Only publicly available information from the company websites was examined. This information can be viewed and possibly exploited by all web users. The analyzed attack scenarios include SSL and TLS encryption analyses, as well as fingerprinting for frameworks used and scans for open ports.

TABLE OF CONTENTS

SUMMARY

The Crashtest Security study found that 50% of companies have more than 7 vulnerabilities in their web presence and 2,668 companies have at least one vulnerability with a critical or high CVSS score. In an analysis by industry, large companies or companies from the aerospace industry in particular turned out to be the most secure categories. In mechanical engineering in particular, there is a need to catch up in terms of web application security.

Our recommendations from the results of the study include:

+ Immediate elimination of the critical security gaps
+ Create an internal update and emergency plan
+ Use automated security scans
+ Closing all open ports that are not needed

1. IMPORTANCE OF CYBER SECURITY FOR COMPANIES

Although every entrepreneur is aware of the importance of cyber security, the topic is still mostly treated stepmotherly. Many companies do not have a clear strategy let alone defense mechanisms against attacks from the web. Reports such as the theft of sensitive bank data by skilled individuals[1], encryption of the entire company or organizational data by ransomware of small, unknown hacker groups[2] or espionage attacks by (sometimes even state-sponsored) hacker groups from China[3] are commonplace today.

The massive data leak from the Marriott hotel chain, through which 500 million customer records were stolen[4] , or the remarkable ransomware attack on Norsk Hydro[5] , which was not paid for, are the two most prominent cases of recent times and show that the economic damage suffered by companies can even threaten their very existence. Today, hackers are increasingly using tools for automated attacks, which once again significantly increase the reach of such attacks and also endanger companies that would otherwise not be a target of such attacks[6].

How well is German industry equipped to deal with these attacks? After all, 54% percent of companies in Germany have had a specific IT security incident in the last two years (2018)[7] and today a large part of the value creation of many companies depends directly or indirectly on digital, networked processes. This study addressed this issue by taking a close look at the online presence of 5,353 companies and examining them according to their security standards. This reveals how well German industrial companies monitor and control the security of their web presences, whether there are differences between industrial sectors, and whether large, international corporations are better secured than small and medium-sized enterprises (SMEs).

2. CONDUCTING THE STUDY

Crashtest Security, as the leading German provider of automated vulnerability analysis, has examined only publicly available information of the company websites for this analysis. This information can be viewed and possibly exploited by all web users. No invasive testing of computer systems or scans of IT infrastructure were performed, which would provide a more complete picture of cybersecurity but cannot be performed at these scales for ethical and legal reasons. Similar scans have already been performed to evaluate the prevalence and resilience of protocols in use, such as SSH[8] and DNS[9].

CVSS ASSESSMENT

All information is evaluated in a standardized way to assess the risk of potential vulnerabilities. The Common Vulnerability Scoring System (CVSS v3.0, https://www.first.org/cvss/) is used for this purpose. CVSS is an industry standard for assessing the risk of a security vulnerability of IT systems. CVSS allows different security vulnerabilities to be assessed and compared using a questionnaire. The CVSS value can be translated into a qualitative risk assessment. This identifies the following values:

STATUS	BASE VALUE
INFO	0
LOW	0.1 - 3.9
MEDIUM	4 - 6.9
HIGH	7 - 8.9
CRITICAL	9 - 10

This assessment helps companies to evaluate the risks of security gaps and integrate them into internal risk management processes. For example, security gaps with a high and critical rating should be closed as immediately as possible. In contrast, a rating of 0 means that there is no concretely identifiable risk. This rating is often used to indicate information that needs to be verified by the user, e.g., a port scan to check whether the port must be open or is sufficiently secured.

This study evaluates information that was publicly available on the websites of companies that deploy web applications on their own without performing an attack on them. The following information is evaluated:

SSL/TLS SCAN

The scan attempts to establish an SSL/TLS connection to the target site by sending connection requests with different protocol versions and encryption algorithms one after the other.

Based on the responses, it can be evaluated whether a secure HTTPS connection can be established with current TLS protocol and secure encryption algorithm.

FINGERPRINTING

By calling the target page, the HTML code and the header of the response are examined for typical detection features of the software and program libraries used. If one is found, the version used is checked against the CVE database (Common Vulnerabilities and Exposures, https://cve.mitre.org/) of known vulnerabilities to make an assessment of any known vulnerabilities.

If no vulnerability is known, a default value of 5.3 is set, as this still represents a „Sensitive Information Disclosure“ vulnerability.

PORTSCAN

The scan tries to connect to the 1,000 most frequently used ports on the server of the target site. Here it is tested whether, in addition to standard ports such as 80 (HTTP) and 443 (HTTPS), database ports are also open through which an attacker can gain unauthorized access to the database, for example to read out customer data.

A total of 40 security vulnerabilities were used to analyze the websites (Table 1, see also Appendix 1).

The following were excluded from the the following identified security vulnerabilities:

SSL NOT AVAILABLE:

If no SSL/TLS connection could be established, this is assessed by the security scanner as a high security vulnerability (CVSS value: 7.4; CVSS vector: AV:N/AC:H/PR:N/UI:N/S:U/C:H/ I:H/A:N). In that case, the fingerprinting scanner does not provide reliable results because it cannot connect to the target page. This affects 577 tested pages..

ALL RESULTS REPORTED BY THE SECURITY SCANNER WITH A CVSS VALUE OF 0.0

This applies to the port scanner, for example, if it detects open ports such as port 22. Without knowledge of the systems, it is not possible to evaluate whether this port must be open to the outside (e.g., to establish an SSH connection) and is appropriately secured. Regardless of this, ports that allow a database connection, such as 3306 (MySQL), were included in the further analysis as a security vulnerability. Although it is also not possible to directly assess whether this port is deliberately open, these were nevertheless considered further due to massive attacks and security incidents on unprotected databases[10].

Table 1: Results of the analysis

3. RESULTS OF THE ANALYS

Vulnerability	CVSS	Vulnerability	CVSS
Portscanner	0,0	SSL Session	4,8
SSL CAA Record	0,0	Heartbleed	5,0
SSL / TLS Warning	0,0	Fingerprint Web Application Framework	5,3
OCSP Stapling	2,2	Fingerprint Web Server	5,3
SSL CRIME	2,6	SSL Secure Renegotiation	5,8
SSL POODLE	3,1	SSL SWEET32	5,9
SSL Cipher Block Chaining SSL3	3,1	SSL DROWN	5,9
SSL Cipherlist AVERAGE	3,7	SSL ROBOT	5,9
SSL LOGJAM Common Primes	3,7	TLS Fallback SCSV	6,5
SSL LOGJAM	3,7	SSL Perfect Forward Secrecy	6,5
SSL Beast	4,3	SSL Cipherlist 3DES IDEA	7,4
SSL Cipher Block Chaining TLS1	4,3	SSL TRUST	7,4
SSL RC4	4,3	SSL Encryption Missing	7,4
SSL FREAK	4,3	SSL Cipherlist LOW	7,4
Missing HSTS	4,8	Certificate Revocation	7,4
Missing Security Headers	4,8	SSL Protocol Version	8,2
TLS Configuration	4,8	SSL Cipherlist STRONG	9,1
SSL Cipher Order	4,8	SSL Cipherlist EXPORT	9,1
SSL Insecure Algorithm	4,8	SSL Cipherlist aNULL	9,1
TLS Key Size	4,8		

3.1 OVERVIEW OF THE BASIC POPULATION

In total, 5,353 online presences of companies listed in German industrial associations from five sectors were scanned (cf. member associations of the BDI[11]): Automotive, Mechanical Engineering, Chemical Industry, Aerospace and Plastics Industry. The different industry structure is responsible for the fact that more than half of the websites belong to the mechanical engineering industry, which is characterized by many very small companies.

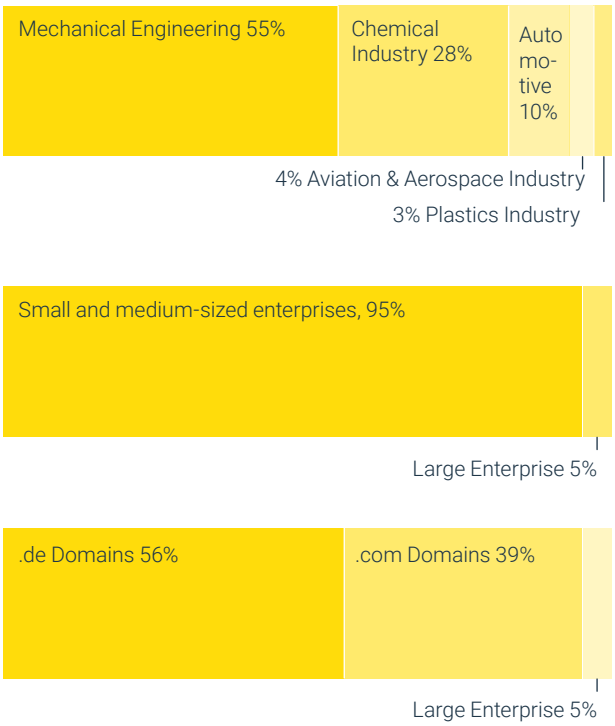
These branches represent a large part of the value creation and innovative power of German industry, which makes them particularly interesting for hacker attacks. 270 companies (5%) were identified as representing the innovative power of German industry based on their revenue (>2 billion) and global presence (Europe, North America, and Asia), making them particularly interesting for hacker attacks. 270 companies (5%) were classified as large corporations based on their revenue (>2 billion) and global presence (Europe, North America, and Asia), i.e., companies such as BMW, Siemens, BASF, GEA, or Airbus. However, only about half of the websites (56%) were listed in the German top-level domain .de, as many companies belong to foreign parent companies or prefer an international online presence themselves. However, this is irrelevant for this study, as security must of course be provided regardless of the top-level domain and is the responsibility of the respective company.

10% **OF WEBSITES STILL COMMUNICATE USING OUTDATED HTTP PROTOCOLS.**

3.2 USE OF HTTP PROTOCOLS

One of the most fundamental elements of a secure online presence is the use of HTTPS protocols for secure communication between endpoints. HTTPS has been the general standard on the web for several years. This makes it all the more surprising that around 10% of websites still communicate using outdated HTTP protocols (see Figure 1). However, there are large differences between the industries with the aerospace industry as the industry with the lowest use of old HTTP protocols.

Figure 1: Composition of the sample pool (n = 5,353) according to...



For further analysis, the websites without HTTPS protocols (577 websites) were excluded because they would distort the statistics (see page 5, „SSL not available“).

3.3 NUMBER OF VULNERABILITIES FOUND AND CVSS SCORE PER INDUSTRY

Across the industry, an average of 7.9 vulnerabilities were found per website scanned with an average CVSS score of 6.7 per website. The industries can thus be divided into three groups:

+ Sicherheits-Vorreiter mit wenig gefunden Schwachstellen und geringem CVSS-Wert (Luft- und Raumfahrt)
+ Sicherheits-Mitläufer mit durchschnittlicher Anzahl gefundener Schwachstellen und durchschnittlichem CVSS-Wert (Kunststoffindustrie, Automotive und Chemische Industrie)
+ Sicherheits-Nachzügler mit überdurchschnittlich vielen gefunden Schwachstellen und hohem CVSS-Wert (Maschinenbau)

The type of vulnerabilities found also differs to a small extent between industries. For example, the automotive and aerospace industries have far fewer fingerprint findings, which suggests more disciplined behavior in dealing with paches and updates. However, the automotive industry has the most SSL findings, in which the aerospace industry again scores best. The plastics industry, on the other hand, has a particularly high number of open ports with database access.

Large corporations perform better than SMEs, presumably because they usually have more resources and expertise available for cyber security departments. Large corporations have about one fewer vulnerability per company and a CVSS score that is about 0.2 points lower.

Once again, the mechanical engineering industry performs worst and the aerospace industry best in all three categories. The above-average number of open ports in the plastics industry and the few fingerprint findings from the automotive and aerospace industries also appear remarkable. According to the study, these industries are the most consistent in downloading patches, while the plastics industry lags behind the others in the topic. Fingerprinting findings that have identified frameworks in use that have a known, exploitable vulnerability are among the most serious.

30.4% of the companies surveyed have such a vulnerability and, again, mechanical engineering performs worst with 33% of companies in contrast to aerospace with 25.8% and plastics with 24.5%.

There are some differences between industries in the use of HTTPS protocols, the average number of vulnerabilities per company, and the average CVSS score. However, overall the differences are rather small with only a few percentage points difference to an overall average that is much too high. With little effort from any company, this could be significantly reduced in any industry.

3.4 THE MOST SERIOUS AND WIDESPREAD VULNERABILITIES

Regardless of the industry, some vulnerabilities are very widespread (Table 2). Although these most widespread vulnerabilities often do not have a high CVSS value, the vulnerabilities with a high CVSS value are also found in too many companies (Table 3).

30% **OF COMPANIES USE SOFTWARE COMPONENTS WITH SECURITY VULNERABILITIES**

Table 2: Overview of the most widespread vulnerabilities

Vulnerability	Amount	CVSS Value	Businesses
SSL Cipherlist AVERAGE	4686	3,7	87%
Fingerprint Web Application Framework	4465	5,3	52%
Missing HSTS	4074	4,8	76%
SSL Beast	3934	4,3	73%
SSL Cipher Block Chaining TLS1	3934	4,3	73%
OCSP Stapling	3280	2,2	61%
TLS Configuration	3039	4,8	52%
Missing Security Headers	2792	4,8	33%
CVE-finding	1637	4,3-10,0	30%
SSL Cipherlist 3DES IDEA	1512	7,4	28%

On the sites of 30% of the companies, a security vulnerability was discovered in a software component used, for which a CVE entry exists. Such vulnerabilities are very easy for attackers to discover, since the CVE database can be searched for the software version used. There is even a complete attack class - Google Hacking - which uses search engines to try to discover vulnerable systems[12]. These gaps can usually be fixed with a simple software update.

At 28% of organizations, nearly a third use an SSL/TLS version with the 3DES algorithm. This algorithm was circulated in 1998 and AES was introduced as its successor as early as 2001. As of 2017, 3DES is considered obsolete[13]. A few companies additionally have SSL/TLS in use, which does not allow to choose a secure encryption algorithm (SSL Cipherlist STRONG), offers weak (SSL Cipherlist LOW), very weak encryption algorithms (SSL Cipherlist EXPORT) or SSL/TLS without encryption (SSL Cipherlist aNULL).

For about 15% of the companies, it is not possible to check the server identity against the issued certificate, resulting in a warning in the browser (Figure 4) when the page is accessed.

3% of the companies have neither a Certificate Revocation List (CRL) nor an Online Certificate Status Protocol (OCSP) defined for their server. As a result, they have no way to revoke their certificates if the associated secret key is stolen. Attackers who come into possession of the certificate can thus imitate the site without being prevented by the SSL/TLS certificate.
A detailed description of the individual vulnerabilities can be found in our Wiki on the Crashtest Security website (https://wiki.crashtest-security.com).

In a further analysis, the vulnerabilities were each classified as critical, high, medium, low and none as mentioned above. This classification provides a quick overview of the current security status of your own web presence.

7,5% **OF COMPANIES HAVE AT LEAST ONE CRITICAL VULNERABILITY**

Table 3: Overview of vulnerabilities with the highest CVSS value

Vulnerability	Amount	CVSS value	Businesses
CVE-finding	1637	4,3-10,0	30%
SSL Cipherlist STRONG	141	9,1	3%
SSL Cipherlist EXPORT	12	9,1	0%
SSL Cipherlist aNULL	8	9,1	0%
SSL Protocol Version	415	8,2	4%
SSL Cipherlist 3DES IDEA	1512	7,4	28%
SSL TRUST	1214	7,4	15%
SSL Cipherlist LOW	304	7,4	6%
Certificate Revocation	167	7,4	3%
TLS Fallback SCSV	288	6,5	5%

7,9%

AVERAGE NUMBER OF VULNERABILITIES PER COMPANY

Applied to the population (Figure 2) shows that 7.5% of the companies have at least one critical vulnerability, 60.6% of the companies have at least one critical or highly rated vulnerability. Only 2.3% of companies, on the other hand, have at most vulnerabilities classified as low. 60.6% companies must therefore be classified as highly vulnerable to automated cyber attacks, or only 2.3% are adequately protected.

It can be seen that the security vulnerabilities with lower risk occur more frequently than the vulnerabilities with high risk. Nevertheless, pages make themselves vulnerable to attack, for example, by disclosing version information about the software used (fingerprint-web-application-framework).
If a security vulnerability becomes known for one of the software components used, these sites are very quickly the target of an attack.
Additional protection mechanisms such as HSTS or security headers, such as a content security policy, are also insufficiently in use. Not only the CVSS value, but also the number of vulnerabilities per company varies greatly by an average of 7.9 vulnerabilities per website.

FIGURE 2: NUMBER OF COMPANIES PER VULNERABILITY CLASSIFICATION

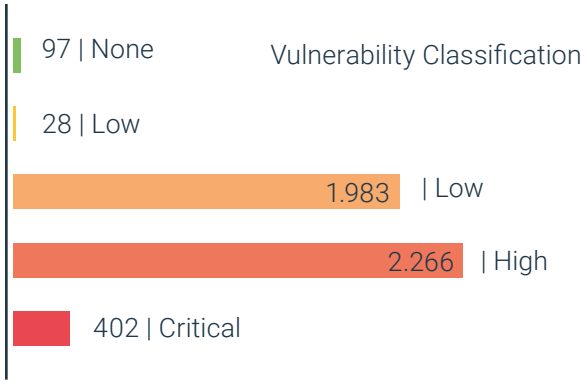
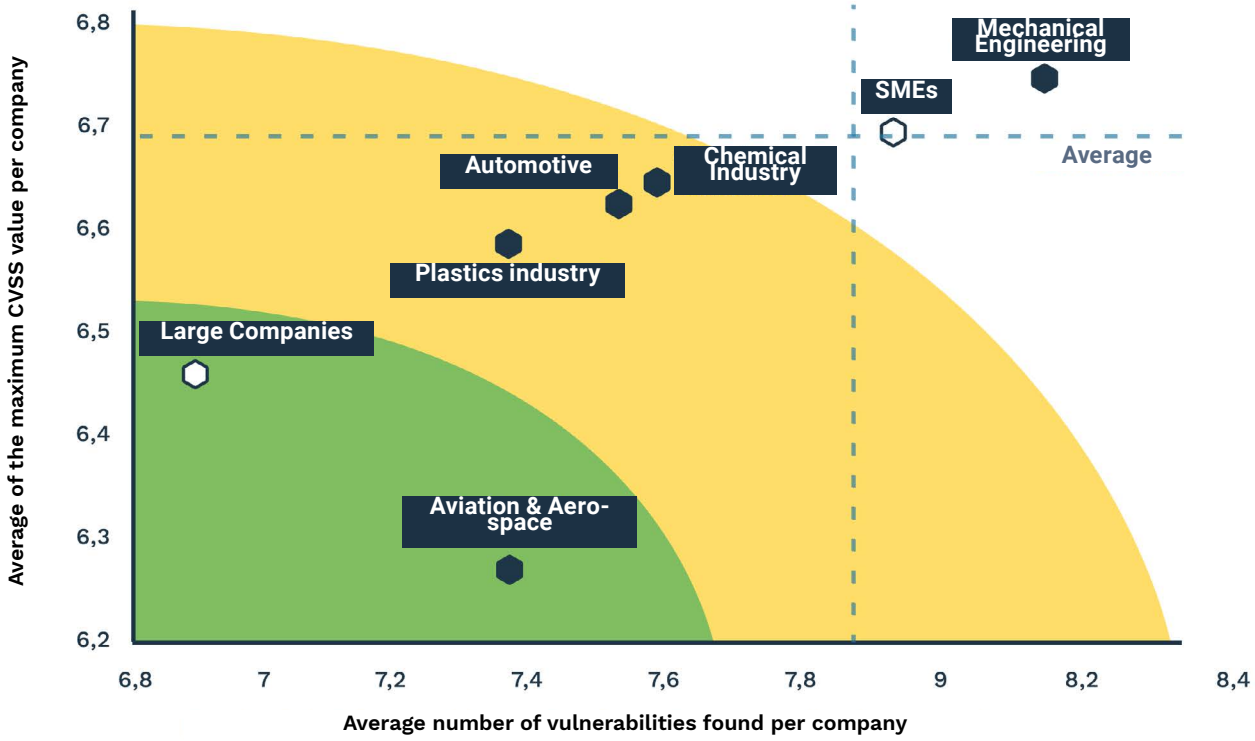


FIGURE 3: OVERVIEW OF THE AVERAGE CVSS-VALUE AND NUMBER OF VULNERABILITIES PER COMPANY



39 **MAXIMUM VULNERABILITIES FOUND PER COMPANY**

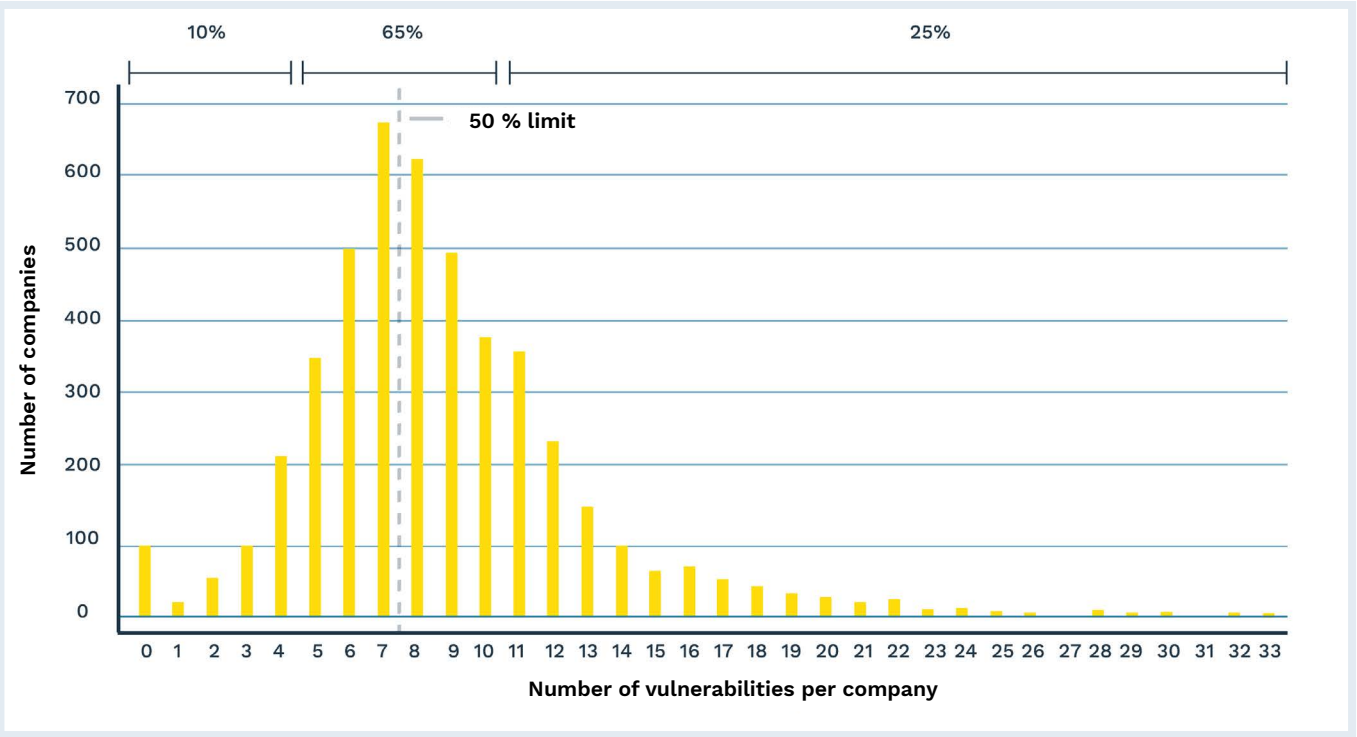
50% **OF COMPANIES HAVE MORE THAN 7 SECURITY VULNERABILITIES**

2668 **NUMBER OF COMPANIES WITH AT LEAST ONE HIGH OR CRITICAL CVSS RATING**

Only 97 companies have no vulnerabilities with a CVSS value greater than 0. The top performer had a total of 39 vulnerabilities, which require a great deal of effort to close. 10% of the companies have less than 5 vulnerabilities, another 65% have between 5 and 10 vulnerabilities. This means that in about 25% of the examined websites have more than 10 vulnerabilities on their website, which can be used as a gateway for a cyber attack with more or less effort.

In summary, regardless of the industry, in about 50% of the companies have more than 7 vulnerabilities in their web presence and 2,668 companies have at least one vulnerability with a critical or high CVSS value that requires immediate action.

Figure 4: Number of vulnerabilities per company



4. STRATEGIC DERIVATIONS

In summary, it can be said that there are considerable gaps in the cyber security of most German industrial companies. Differences between the industries are present, with the aerospace industry as the most secure industry, but marginal. Hackers using automated tools will find vulnerabilities to attack in the majority of companies. However, cybersecurity can be significantly improved by any company with few steps and few resources. Crashtest Security recommends the following steps on the path to increased cyber security:

1. USE OF SECURITY SCANS

Vulnerabilities in web applications cannot be completely avoided in development, especially with the numerous releases in agile software development. To make these vulnerabilities visible to developers, security tests of the finished system are inevitable. A single scan or a manual pentest quickly reveals the most important vulnerabilities. For constant security, however, automated security scans must not be missing, because only with their help can each new release be checked for vulnerabilities.

2. IMMEDIATE MITIGATION OF THE CRITICAL SECURITY GAPS:

If the security tests have found particularly critical vulnerabilities (CVSS value > 7.0), it is advisable to close them immediately! Because, as explained above, they represent a serious business risk for the entire company. Closing them is the most urgent step. This is the only way to fend off automated attacks that are not specifically directed against your own company, but have accidentally landed on your own company's online presence as part of a mass attack.

3. CREATE AN INTERNAL UPDATE PLAN:

Another popular way into the internal areas of a company are, as mentioned above, outdated frameworks of a website where security gaps are already known. Such gaps are still constantly being found and exploited until they are generally known and closed by all providers. An internal update plan with clear processes and responsibilities is a key to preventing frameworks from becoming obsolete and insecure during operation.

4. CLOSE ALL OPEN PORTS THAT ARE NOT NEEDED:

An open port that was once forgotten by the developers can still become a gateway for attacks from the web years later. Therefore, on the one hand, all unnecessary ports should be closed, and on the other hand, those that absolutely must be open should be strictly regulated and constantly controlled.

5. CREATION OF AN EMERGENCY PLAN

However, the inescapable truth is that the risk of falling victim to a hacker attack can never be completely eliminated. A sophisticated contingency plan with backup strategy and behavioral plan in case of an attempted/successful attack are essential to continue to ensure a company's IT operations and to keep the damage as low as possible. For more information on contingency plans, see also related articles at Security Insider[14].

KEY TAKEAWAYS F0R CISOS

+ No matter what industry you‘re in, your company is very likely to have some vulnerabilities to cyberattacks.
+ Complete security is not possible, so a contingency plan is an important part of your business strategy.
+ Responsibilities must be clearly defined and assigned so that necessary steps such as disciplined update behavior and management of open ports can be carried out.

KEY TAKEAWAYS FOR ENTWICKLER

+ Automated testing tools make it possible to detect and close vulnerabilities before they are released, before they become an acute gateway.
+ Disciplined behavior in updating frameworks and managing ports is essential for the security of the entire website.
+ In an emergency, action must be taken quickly, and the necessary steps must be discussed and coordinated in advance so that the response can be fast and flexible.

KEY TAKEAWAYS FOR QM

+ To prevent data leaks, transparency about the security status of one‘s own web applications is essential.
+ In order to obtain transparency about the own security status, security scans of the own web presences are inevitable.
+ In addition to selective manual pentests, automated testing tools are particularly necessary because they guarantee a continuously high security level.

CRASHTEST SECURITY GMBH

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

info@crashtest-security.com

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

SOURCES:

[1] Michael Maisch, Felix Holtermann, Christof Kerkmann, Astrid Dörner (2019): „Hackerangriffe sorgen für Zweifel an Clouds für Banken“ in Handelsblatt. URL: https://www.handelsblatt.com/finanzen/banken-versicherungen/banken/datenklau-hacker-angriffe-sorgen-fuer-zweifel-an-clouds-fuer-banken/24860660.html

[2] Deutsche Presseagentur (2019): „Cyber-Attacke auf Kliniken: Schwachstelle war ‚altes Dienstkonto‘“ in heise online. URL: https://www.heise.de/newsticker/meldung/Cyber-Attacke-auf-Kliniken-Schwachstelle-war-altes-Dienstkonto-4502412.html

[3] Ute Ross (2019): „Doppelbedrohung: Chinesische APT-Gruppe spioniert für Staat und bereichert sich“ in heise online. URL: https://www.heise.de/ix/meldung/Doppelbedrohung-Chinesische-APT-Gruppe-spioniert-fuer-Staat-und-bereichert-sich-4492698.html

[4] Maria Armental (2019):“Marriott Takes $126 Million Charge Related to Data Breach” in The Wall Street Journal. URL: https://www.wsj.com/articles/marriott-take-126-million-charge-related-to-data-breach-11565040121

[5] Joe Tidy (2019): “How a ransomware attack cost one firm £45m” in BBC News. URL: https://www.bbc.com/news/business-48661152

[6] Robert Krenn (2019): „The Rise of Automated Hacking“ in Infosecurity Magazine. URL: https://www.infosecurity-magazine.com/infosec/the-rise-of-automated-hacking-1-1-1/

[7] BMWI (2019): “Den digitalen Wandel gestalten“, online Veröffentlichung des Bundesministeriums für Wirtschaft und Energie. URL: https://www.bmwi.de/Redaktion/DE/Dossier/digitalisierung.html

[8] Ralph Holz, Johanna Amann, Abbas Razaghpanah, Narseo Vallina-Rodriguez (2019): “The Era of TLS 1.3: Measuring Deployment and Use with Active and Passive Methods”. URL: https://arxiv.org/pdf/1907.12762.pdf

[9] Patrick Sattler (2019): “Large-Scale DNS Analysis, Master Thesis TUM”. URL: https://media.net.in.tum.de/videoarchive/WS18/Oberseminar/2019+01+14_1708+Large+Scale+DNS+Analysis/priv/slides.pdf

[10] Catalin Cimpanu (2019): “MongoDB databases still being held for ransom, two years after attacks started in Zero Day Net”. URL: https://www.zdnet.com/article/mongodb-databases-still-being-held-for-ransom-two-years-after-attacks-started/
Für eine Übersicht der Betroffenen siehe auch: https://docs.google.com/spreadsheets/d/1QonE9oeMOQHVh8heFIyeqrjfKEViL0poLnY-8mAakKhM

[11] Bundesverband der deutsche Industrie e.V. (2019): „Mitgliederliste des BDI“. URL: https://bdi.eu/der-bdi/mitglieder/

[12] Jonny Long, Jeff Steward, Petko D. Petlov, Ryan Langley (2008). “Google Hacking for Penetration Testers Volume 2”.

[13] National Institue of Standards and Technology (2017): “Update to Current Use and Deprecation of TDEA”. URL: https://csrc.nist.gov/News/2017/Update-to-Current-Use-and-Deprecation-of-TDEA

[14] Stefan Luber, Peter Schmitz (2017): „Was ist ein IT-Notfallplan?“ in Security Insider. URL: https://www.security-insider.de/was-ist-ein-it-notfallplan-a-648745/

Vulnerability	CVSS	Description
Fingerprint Web Application Framework	5,3	The installed web application framework(s) offer information about their version. This opens attackers the possibility to look for exploits specifically targetting the software running in its exact version.
Fingerprint Web Server	5,3	The webserver publicly provides information about itself such as the name or version. This opens attackers the possibility to look for exploits specifically targetting the webserver in its exact version.
Portscanner	0,0	Unneeded open ports on the webserver open a large attack surface to a malicious user. This can be used to find unmaintained and possibly vulnerable network services that can be targeted.
SSL Insecure Algorithm	4,8	The used encryption algorithm has severe security issues.
SSL BEAST	4,3	The server is vulnerable for BEAST (Browser Exploit Against SSL/TLS) attacks. By using weaknesses in cipher block chaining, an attacker can use a Man-In-The-Middle attacks to decrypt and obtain authentication tokens.
SSL CAA Record	0,0	DNS Certification Authority Authorization (CAA) Resource Record / RFC6844: Not offered
SSL Cipher Block Chaining SSL3	3,1	The webserver is configured to allow connections encrypted with SSL V3 in Cipher Block Chaining Mode (CBC). Connections using this settings contain predictable information that allow an attacker to break the encryption using the BEAST attack.
SSL Cipher Block Chaining TLS1	4,3	The webserver is configured to allow connections encrypted with TLS V1 in Cipher Block Chaining Mode (CBC). Connections using this settings contain predictable information that allow an attacker to break the encryption using the BEAST attack.
SSL Cipherlist 3DES IDEA	7,4	The server is configured to support 3DES and IDEA Ciphers like „3DES:IDEA“. This means, that an attacker can make use of an insecure SSL/TLS connection.
SSL Cipherlist aNULL	9,1	The server is configured to support anonymous NULL Ciphers like „aNULL:ADH“, which allow non authenticated traffic. This means, that an attacker can make use of an insecure SSL/TLS connection.
SSL Cipherlist AVERAGE	3,7	The server is configured to support average Ciphers like „HIGH:MEDIUM:AES:CAMELLIA:ARIA“. This means, that an attacker can make use of an insecure SSL/TLS connection.
SSL Cipherlist EXPORT	9,1	The server is configured to support EXPORT Ciphers like „EXP:EXPORT:EXPORT40:EXPORT56“. All EXPORT ciphers use a very short key size and are therefore very weak.
SSL Cipherlist LOW	7,4	The server is configured to support low Ciphers like „LOW:DES:RC2:RC4“. This means, that an attacker can make use of an insecure SSL/TLS connection.

Vulnerability	CVSS	Description
SSL Cipherlist STRONG	9,1	The server is NOT configured to support Strong Ciphers like „AESGCM:CHACHA20:AESGCM:CamelliaGCM:AESCCM8:AESCCM“. By not using strong ciphers, the send traffic can be decrypted in a shorter time.
SSL CRIME	2,6	The server is vulnerable for CRIME (Compression Ratio Info-leak Made Easy) attacks. The attack against secret web cookies sent over compressed HTTPS or SPDY connections, leaves cookie data vulnerable to session hijacking.
Certificate Revocation	7,4	The webserver is badly configured regarding revoked certificates. Certificate Revocation Lists (CRLs) and the Online Certificate Status Protocol (OCSP) make sure, that users can verify the integraty of a server certificate.
SSL DROWN	5,9	The server is vulnerable for DROWN (Decrypting RSA with Obsolete and Weakened encryption) attacks. The TLS protocol suite supports the insecure SSL v2 protocol and attacks using this vulnerability can leak the session key for a captured TLS handshake.
TLS_FALLBACK_ SCSV	6,5	The TLS Signaling Cipher Suite Value (SCSV) is a protection against TLS/SSL downgrade attacks. The server is vulnerable as it establishes a connection to the client with a weak protocol version even when the TLS_FALLBACK_SCSV value is set in the client request.
SSL FREAK	4,3	The server is vulnerable for FREAK (Factoring RSA Export Keys) attacks. Due to a weakness in the SSL/TLS protocols using only 512 or less bits it can easily be broken.
TLS Configuration	4,8	There is a misconfiguration with your SSL/TLS configuration. SSL/TLS is responsible for encrypting traffic between your web application and a user‘s browser to prevent eavesdropping.
Heartbleed	5,0	The used OpenSSL cryptography library is vulnerable to heartbleed. Abusing this vulnerability, an attacker may be able to steal the private key of the server certificate.
Missing HSTS	4,8	The webserver does not offer HTTP Strict Transport Security (HSTS). HSTS enforces HTTPS connections, which prevents downgrade attacks to an insecure HTTP connection.
TLS Key Size	4,8	The security of a TLS connection heavily depends on the used keysize. The server offers a keysize which will result in a weak encryption.
SSL LOGJAM	3,7	The server is vulnerable for LOGJAM, a security vulnerability against a Diffie-Hellman key exchange using 512 to 1024 bit keys. The attack forces a downgrade on the TLS connection to use only 512 bits which allows to read and inject data into the connection.
SSL LOGJAM Common Primes	3,7	The server is vulnerable for LOGJAM, a security vulnerability against a Diffie-Hellman key exchange using 512 to 1024 bit keys. The algorithm uses in most cases the same pregenerated prime numbers which makes it way easier (and cheaper) to crack such an encryption.

Vulnerability	CVSS	Description
SSL Encryption Missing	7,4	There is no SSL/TLS encryption enabled on your server. All traffic to your web application is transported via unencrypted channels. This leaves your users vulnerable to man-in-the-middle attacks.
OCSP Stapling	2,2	OCSP Stapling is disabled on your server. Therefore, your certificate authority might track which users visit your site.
SSL Cipher Order	4,8	There is no cipher order for HTTPS ciphers set or the cipher order includes an insecure cipher. This means, that an attacker can make use of an insecure SSL/TLS connection.
SSL Perfect Forward Secrecy	6,5	Perfect Forward Secrecy is unavailable with the server configuration. If the TLS encryption is broken once, recordings of previous connections are not secure and may be decrypted.
SSL POODLE	3,1	The server is vulnerable for POODLE (Padding Oracle On Downgraded Legacy Encryption) attacks. With the Man-In-The-Middle attack using the SSL 3.0 Fallback, an attacker can expose data of encrypted connections.
SSL Protocol Version	8,2	A SSL/TLS version offered by the server is outdated. The deprecated versions contain weak implementations that cannot be considered as secure anymore.
SSL RC4	4,3	The server supports RC4 (Rivest Cipher 4), which is a cipher stream that is considered insecure due to multiple known vulnerabilities.
SSL ROBOT	5,9	The server is vulnerable for ROBOT (Return of Bleichenbacher's Oracle Threat), a security vulnerability against cipher suites using the RSA algorithm. An attack exploiting this vulnerability can fully break the confidentiality of the encryption.
Missing Security Headers	4,8	Security headers can effectly prevent certain hacking attempts. You should consider headers like Strict-Transport-Security, Content-Security-Policy, X-Frame-Options or X-XSS-Protection
SSL Secure Renegotiation	5,8	The renegotiation process of the SSL encryption is vulnerable. It allows two negotiations (one before the renegotiation, and one after) to be handled by different parties. This leaves the data vulnerable to Man-In-The-Middle attacks.
SSL Session	4,8	The TLS session resumption functionality is misconfigured. This opens attackers the possibility to steal existing TLS sessions from other users.
SSL SWEET32	5,9	The server uses short block sizes, which makes it vulnerable to hit the same hash for multiple inputs. By observing the data for a longer period of time, an attacker can recover secure HTTP cookies.
SSL Trust	7,4	The X.509 certificate issued for this domain cannot be trusted. Clients such as browsers will show warnings or not be able to connect if they cannot trust the certificate. Trust issues arise if the common name in the certificate does not match the webserver domain or if the certificate is selfsigned.

Vulnerability	CVSS	Description
SSL/TLS Warning	0,0	Your website produces a SSL/TLS warning. A warning from the SSL/TLS scanner does not indicate a direct vulnerability, but highlights a potential issue that needs to be manually reviewed.