

INDUSTRIAL SECURITY THREAT RANSOMWARE: WHAT CAN YOU DO NOW?

Almost every day, well-known companies find themselves in the headlines because they have been the victim of a [cyberattack](#). For a long time now, security training and the development of measures have no longer been about the question of whether one will be affected, but when and to what extent. However, this does not mean that [manufacturing companies](#) should just sit and wait until the time comes. They can take a number of [precautions](#) to delay attacks and be as resilient as possible to attacks. Moreover, even after a security attack, the right measures can [minimize the damage](#).

The first step is to create [awareness](#) within the company. Not only the security officers should deal with the topic, but also the [employees](#). Because when attackers want to gain access to data, they often do so via employees through [social engineering](#).

We have already supported many customers in their [company-specific security training](#). With this paper, we offer manufacturing companies an [exclusive insight](#) into our training content in order to give them a jump-start on the topic of industrial security, especially [ransomware](#).

WHAT YOU WILL LEARN IN THE PAGES AHEAD:

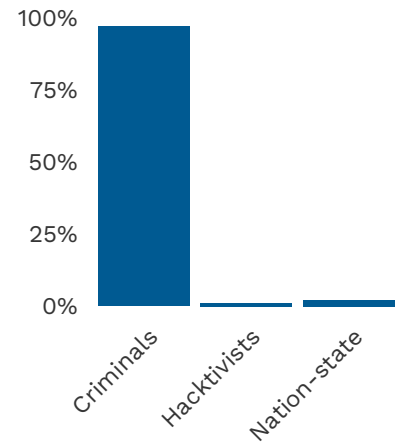
- | | |
|--|---|
| 1. Facts and figures on the current threat situation | 2 |
| 2. Typical course of a ransomware attack: via phishing email | 3 |
| 3. Tips: What can you do in advance? | 4 |
| 4. Conclusion | 5 |

1. FACTS AND FIGURES ON THE CURRENT THREAT SITUATION

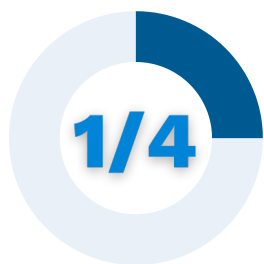
9/10

companies are affected by cyberattacks.

97 %
of all cyberattacks originate from **CRIMINALS**.



25 %
of the attacks in Europe are directed to **MANUFACTURING COMPANIES**.



This makes them the **NUMBER 1** target in 2021.

In 2018, manufacturing companies were still ranked **NUMBER 8**

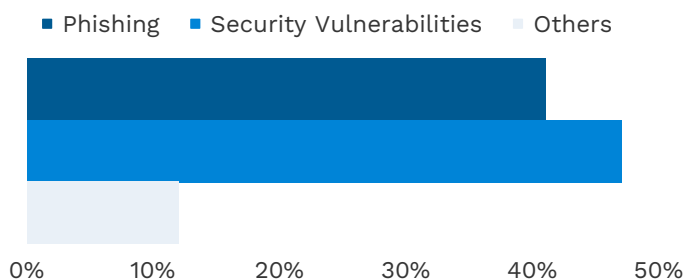
21 %

of those attacks are **RANSOMWARE ATTACKS**.

In the field of **OPERATIONAL TECHNOLOGIES** even



Why do these attacks happen?




CONCLUSION:


88 % of all attack could have been prevented by


1. Security **MEASURES**
2. Security **TRAININGS**


2. TYPICAL COURSE OF A RANSOMWARE ATTACK: VIA PHISHING EMAIL


41% of ransomware attacks originate in a **phishing email**. This means that attackers gain access to data via **social engineering**. The following is a typical sequence of a ransomware attack via a phishing email:


- 1



A seemingly normal **EMAIL** arrives and is opened.
- 2



The **LINK** or **ATTACHMENT** contained in it is opened. This starts the process.
- 3


The malware is automatically **LOADED** onto the hardware.
- 4


The malware is **EXECUTED**.
- 5


Through **LATERAL MOVEMENT** (further infection), the attacker tries to get to sensitive data and infect even more parts of the system. The more systems are infected, the more difficult it becomes to recover the system and the more likely the victim is to pay.
- 6


Data and systems are **ENCRYPTED**. Encryption can occur within one to two hours on all systems. Sometimes several months pass between the attack and encryption. Therefore, care should be taken to know when the attack occurred in order to recover all data.
- 7


The attacker has reached his goal and demands the **RANSOM**.
- 8


WHAT NEXT?

 1. Do not pay the ransom.
 2. Stay calm.
 3. Take action.

Why not pay ransom?

 1. Probability of another attack high, as the company is seen as easy prey.
 2. Co-financing of further development of the malware.
 3. Motivation for attackers to attack more companies.
 4. No guarantee that decryption will work.

3. TIPS: WHAT CAN YOU DO IN ADVANCE?

In order to prepare for a possible attack in advance and thus be in a position to ward it off or at least keep the damage to a minimum, initial measures can be taken in advance:

Technical measures FOR EMAILS	Technical measures IN THE SYSTEM AND NETWORK	Further measures
Marking external emails	2-factor authentication for systems accessible from the Internet, especially for administrator accounts	Regular backups, including the creation of an offline version
Blocking of potentially dangerous file types	Avoidance of direct remote administration access to internal IT systems	Patch management of operating systems and applications
Deactivation of unsigned Office macros	Isolation of vulnerable legacy systems that can no longer be patched	Sensitization of employees to cybersecurity through awareness training
Rejection of externally delivered emails with sender addresses from your own organization	Network segmentation	Plan discussions and exercises on how to act in the event of an incident

4. CONCLUSION

The fact that 88% of all cyberattacks succeed either via [phishing emails](#) or [security holes](#) clearly shows that [patch management](#) and [trained employees](#) can significantly reduce the risks and negative consequences of an attack. Therefore, there is an urgent need for action in two areas:

- [Technical measures](#) on the part of security officers, as shown in the previous table, are important to prepare a company for a possible attack and to keep damage to a minimum. Companies are well advised to draw up a [security concept](#) and a concrete [emergency plan](#) in advance and to establish internal persons responsible for the topic of industrial security.
- The above infographic shows that 41% of all cyberattacks occur via phishing emails, i.e., [social engineering](#). Employees thus represent a weak point in the security system, especially for manufacturing companies. Simply opening an email can have devastating consequences, in the worst case, even a production stop. As a decisive factor at the beginning of an attack, employees can also proactively prevent it: Closing this security leak can be achieved by [raising awareness](#) and regular [training](#) of all employees.

Contact us if you have a need for company-specific security training:
info@university4industry.com

Read [HERE](#) how a company-specific
Industrial Security trainings can look like.

Interesting sources on this topic:

- [IBM X Force Threat Intelligence Index 2022](#)
- [VDMA Emergency Guide Ransomware](#)

Authors if this article:
Industrial Security Team
of University4Industry

