

INDUSTRIAL SECURITY-BEDROHUNG RANSOMWARE: WAS KÖNNEN SIE SCHON JETZT TUN?

Fast täglich finden sich bekannte Unternehmen in den Schlagzeilen wieder, weil sie Opfer einer **Cyber-Attacke** wurden. Längst geht es in Security-Schulungen und in Maßnahmenerarbeitungen nicht mehr um die Frage, ob man betroffen sein wird, sondern wann und wie stark. Das heißt allerdings nicht, dass **produzierende Unternehmen** tatenlos zusehen sollten, bis es so weit ist. Sie können eine Reihe von **Vorsichtsmaßnahmen** treffen, um Angriffe hinauszuzögern und für Angriffe möglichst resilient zu sein. Außerdem kann auch nach einem Security-Angriff durch die richtigen Maßnahmen der **Schaden minimiert** werden.

Ein erster Schritt ist das Schaffen von **Awareness** innerhalb des Unternehmens. Nicht nur die Security-Beauftragten sollten sich mit dem Thema auseinandersetzen, sondern auch die **Mitarbeiter*innen**. Denn wenn sich Angreifer Zugriff auf Daten verschaffen wollen, tun sie das häufig über Mitarbeiter*innen durch das sogenannte "**Social Engineering**".

Wir haben bereits viele Kunden in ihren **unternehmensspezifischen Security-Trainings** begleitet. Mit diesem White Paper bieten wir produzierenden Unternehmen einen **exklusiven Einblick** in unsere Trainingsinhalte, um ihnen damit eine Starthilfe für das Thema Industrial Security, insbesondere **Ransomware**, zu geben.

WAS SIE AUF DEN KOMMENDEN SEITEN LERNEN:

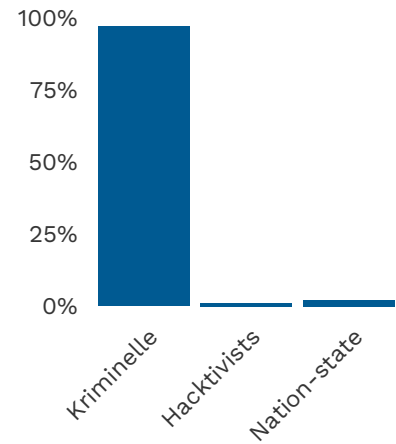
- | | |
|--|---|
| 1. Zahlen und Fakten zur aktuellen Bedrohungslage | 2 |
| 2. Typischer Ablauf einer Ransomware-Attacke: Angriff über Phishing-Mail | 3 |
| 3. Tipps: Was können Sie schon jetzt tun? | 4 |
| 4. Fazit | 5 |

1. ZAHLEN UND FAKTEN ZUR AKTUELLEN BEDROHUNGSLAGE

9/10

Unternehmen sind von Cyberattacken betroffen.

97 %
der Cyberangriffe
gehen von
KRIMINELLEN
aus.



25 %
der Attacken in Europa
richten sich an
PRODUZIERENDE UNTERNEHMEN.



Damit sind sie
im Jahr 2021
Angriffsziel

NUMMER 1

2018 belegten produzierende
Unternehmen noch **PLATZ 8**

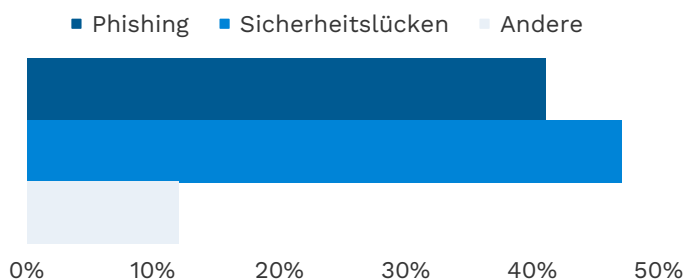
21 %

dieser Angriffe sind
RANSOMWARE-ATTACKEN.

Im Bereich
OPERATIONAL TECHNOLOGIES
passieren sogar



Warum passieren die Angriffe?



FAZIT:

88 % aller Angriffe hätten durch


1. **Security-MASSNAHMEN**
2. **Security-TRAININGS**

vermieden werden können.


2. TYPISCHER ABLAUF EINER RANSOMWARE-ATTACKE: ANGRIFF ÜBER PHISHING-MAIL

41% der Ransomware-Angriffe haben ihren Ursprung in einer **Phishing-Mail**. D.h. über **Social Engineering** verschaffen sich Angreifer Zugang zu Daten. Nachfolgend ein typischer Ablauf eines Ransomware-Angriffs über eine Phishing-Mail:


- 1




Eine scheinbar normale **E-MAIL** kommt an und wird geöffnet.
- 2



Der darin enthaltene **LINK** oder der **ANHANG** wird geöffnet. Dadurch wird der Prozess gestartet.
- 3




Die Schadsoftware wird automatisch auf die Hardware **GELADEN**.
- 4




Die Schadsoftware wird **AUSGEFÜHRT**.
- 5




Durch **LATERAL MOVEMENT** (weitere Infektion), versucht der Angreifer, zu sensiblen Daten zu gelangen und noch mehr Teile des Systems zu infizieren. Je mehr Systeme infiziert werden, desto schwieriger wird es, das System wiederherzustellen und umso höher die Wahrscheinlichkeit, dass das Opfer zahlt.
- 6



Daten und Systeme werden **VERSCHLÜSSELT**. Die Verschlüsselung kann innerhalb von ein bis zwei Stunden auf allen Systemen erfolgen. Manchmal vergehen mehrere Monate zwischen Angriff und Verschlüsselung. Daher sollte man darauf achten, wann die Attacke stattgefunden hat, um alle Daten wiederherstellen zu können.
- 7



Der Angreifer hat sein Ziel erreicht und fordert das **LÖSEGELD**.
- 8



WAS DANN?

 1. Das Lösegeld nicht bezahlen.
 2. Ruhig bleiben.
 3. Maßnahmen ergreifen.

Warum nicht Lösegeld bezahlen?

1. Wahrscheinlichkeit eines weiteren Angriffs hoch, da das Unternehmen als leichte Beute gesehen wird.
2. Mitfinanzierung der Weiterentwicklung der Schadsoftware.
3. Motivation für Angreifer, weitere Unternehmen zu attackieren.
4. Keine Garantie, dass Entschlüsselung funktioniert.

3. TIPPS: WAS KÖNNEN SIE SCHON JETZT TUN?

Um sich bereits im Vorfeld auf eine mögliche Attacke vorzubereiten und damit in der Lage zu sein, diese abzuwehren oder zumindest die Schäden klein zu halten, können im Vorfeld schon erste Maßnahmen getroffen werden:

Technische Maßnahmen BEI E-MAILS	Technische Maßnahmen IM SYSTEM UND NETZWERK	Weitere Maßnahmen
Kennzeichnung externer E-Mails	2-Faktor Authentifizierung bei Systemen, die aus dem Internet erreichbar sind, insbesondere für Administratorkonten	Regelmäßige Backups, inklusive der Erstellung einer Offline-Version
Blockierung potenzieller gefährlicher Dateitypen	Vermeidung direkter Remote- Administrations-Zugänge auf interne IT-Systeme	Patchmanagement von Betriebssystemen und Applikationen
Deaktivierung von unsignierten Office-Makros	Isolation von anfälligen Alt- Systemen, die nicht mehr gepatcht werden können	Sensibilisierung der Mitarbeiter*innen für Cybersicherheit mittels Awareness-Trainings
Ablehnung von extern eingelieferten E-Mails mit Absenderadressen der eigenen Organisation	Netzwerksegmentierung	Planbesprechungen und Übungen, wie man sich bei einem Vorfall verhält

4. FAZIT

Dass 88% aller Cyber-Angriffe entweder über **Phishing-Mails** oder **Sicherheitslücken** gelingen, zeigt eindeutig: **Patch Management** und **geschulte Mitarbeiter*innen** können die Gefahren und negativen Folgen eines Angriffs erheblich senken. Daher herrscht in zwei Bereichen dringend Handlungsbedarf:

- **Technische Maßnahmen** vonseiten der Sicherheitsbeauftragten, wie sie in der vorherigen Tabelle aufgezeigt wurden, sind wichtig, um ein Unternehmen auf einen möglichen Angriff vorzubereiten und die Schäden gering zu halten. Unternehmen sind gut beraten, ein **Sicherheitskonzept** sowie einen konkreten **Notfallplan** im Vorhinein zu erstellen und intern Verantwortliche für das Thema Industrial Security zu etablieren.
- In der oben angeführten Infografik wurde ersichtlich, dass 41% aller Cyberangriffe über Phishing-Mails, also **Social Engineering**, passieren. Mitarbeiter*innen stellen damit insbesondere für produzierende Unternehmen eine Schwachstelle im Sicherheitssystem dar. Denn das einfache Öffnen einer E-Mail kann verheerende Folgen nach sich ziehen: im schlimmsten Fall bis hin zum Produktionsstopp. Als entscheidender Faktor am Beginn eines Angriffs können Mitarbeiter*innen diesen auch proaktiv verhindern: Die Schließung dieses Sicherheitslecks kann durch **Sensibilisierung** und regelmäßiges **Training** aller Mitarbeiter*innen gelingen.

Kontaktieren Sie uns, wenn Sie Bedarf an einem unternehmensspezifischen Security-Training haben: info@university4industry.com

Lesen Sie **HIER**, wie ein unternehmensspezifisches Industrial Security Training aussehen kann.

Interessante Quellen zu diesem Thema:

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

Autor*innen dieses Artikels:
Industrial Security-Team
von University4Industry

