Vodafone Business Education

CYBER SECURITY

Together we can
vodafone
business

Cyberkriminalität

Einige spannende Fakten

Cyberkriminalität ist in den vergangenen Jahren zu einem komplexen illegalen Wirtschaftszweig avanciert. Dabei richten sich die Bedrohungen durch Hacker:innen nicht nur gegen Konzerne, sondern verstärkt auch gegen mittelständische Unternehmen. Denn diese verfügen häufig über Knowhow, das es zu schützen gilt, und zählen in ihren Branchen zu den Hidden Champions. Umso wichtiger ist es also für den Mittelstand, die relevanten Schwachstellen zu kennen und ihnen mit einem Sicherheitskonzept entgegenzuwirken. Diese Aufgabe sollte als Prozess begriffen werden, der nur durch Beteiligung aller Unternehmensebenen zum Erfolg geführt werden kann. Denn egal, ob es sich bei den möglichen Bedrohungsszenarien um Spyware, Ransomware, DoS-Attacke oder Phishing handelt: Ausschlaggebend ist immer der Faktor Mensch. Schulungen, Prozesse und Protokolle für den Ernstfall sind deshalb unverzichtbar.

Der **EINFLUSS VON CYBERCRIME** in Zahlen:

1,81 Mio. €

beträgt der **durchschnittliche Schaden** durch einen Cyberangriff.
Die Schadenssumme ist tendenziell steigend.

Quelle: Bitkom 2022

60 %

der erfolgreichen Cyberangriffe **nutzen Phishing** und somit gültige Nutzerkonten als ersten Angriffsvektor.

Quelle: itsicherheit-online.com 05/2022

88 %

der **deutschen Unternehmen** waren bereits von Datendiebstahl, Industriespionage oder Cybersabotage betroffen.

Quelle: Bitkom 2021

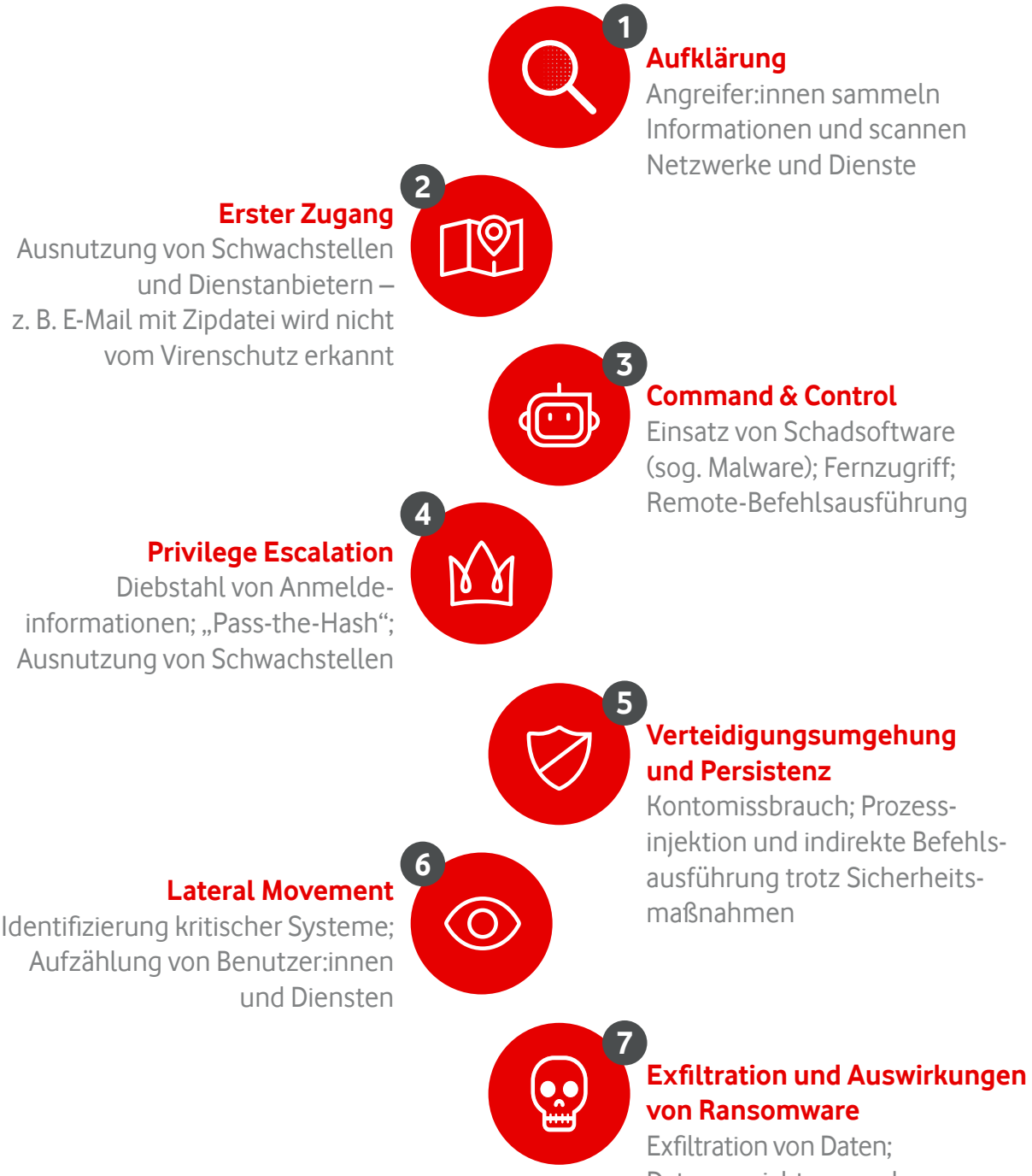
44 %

der Risiko-Management-Expert:innen benennen Cybervorfälle als eines der **Top-3-Risiken** für Unternehmen.

Quelle: Allianz Risk Barometer 2022

Ablauf einer Ransomware-Attacke

Bei einer sogenannten Ransomware-Attacke werden die Daten eines Systems verschlüsselt, um gegen Zahlung eines Lösegelds eine Entschlüsselung in Aussicht zu stellen. Wie der Ablauf einer Ransomware-Attacke aus Sicht cyberkrimineller Täter:innen aussieht, zeigen wir hier:



FÜNF FRAGEN AN ULRICH IRNICH

ULRICH IRNICH
ist **CIO** und **Global Head of Modernisation bei Vodafone Deutschland** sowie Leiter der globalen Organisationseinheit „Digital & IT“. Er verantwortet Zukunftsthemen rund um die Digitalisierung und neue Technologien.

Mehr Infos finden Sie hier.

Warum ist Cyber-Security ein wichtiges Thema?
Wir befinden uns in Deutschland auf dem Höhepunkt von Ransomware-Attacken, die sensible Daten und Lösegeld erpressen. Acht von zehn Unternehmen sind bereits einmal gehackt worden. Es stellt sich daher nicht die Frage, ob ein Unternehmen gehackt wird, sondern wie es darauf vorbereitet ist.

Wie sollte ein Unternehmen mit Cyber-Security umgehen?
Die Geschäftsführung ist die tragende Säule für die Unternehmenssicherheit, daher obliegt es ihrer Verantwortung, für den bewussten und nachhaltigen Umgang mit Kundendaten zu garantieren, ihre Mitarbeitenden zu sensibilisieren und für Awareness zum Thema Cybercrime zu sorgen.

Was sind häufige Cyberattacken? Wo liegen die kritischen Bereiche und Einfallstore?
Wir erleben viele DDoS-Angriffe, aber vor allem Ransomware-Attacken, bei denen Phishingmails an die Mitarbeitenden versendet werden. Durch Social Engineering ist es heute schwierig, die Echtheit von E-Mails zu erkennen. Fehlende Zwei-Faktor- und Multi-Authentifizierungen sowie unsichere Passwörter sind offene Einfallstore für Hacker:innen.

Wie können sich Unternehmen bestmöglich vor Cyberattacken schützen?
Ein Unternehmen, das kein effizientes Backup hat, riskiert schwerwiegende Datenverluste und ist nicht gefeilt gegen Lösegeldforderungen. Daher gilt es, ein effizientes Backup-System zu haben, sodass Daten wiederhergestellt werden können. Bei Vodafone führen wir außerdem Health Checks und Penetration Tests mit Hacker:innen durch, um mögliche Einfallstore zu testen.

Was ist der optimale Cyber-Security-Schutz?
Es ist wichtig, dass alle involviert sind: Cyber-Security ist nicht nur eine Aufgabe der IT-Sicherheit, sondern eine der gesamten Belegschaft. Alle Mitarbeitenden in die Cybersicherheit zu integrieren, die Schwachstellen zu stärken – das ist Aufgabe der Unternehmen.

„DIE AUFGABE VON UNTERNEHMEN IST ES, BEI IHREN MITARBEITENDEN AWARENESS FÜR DAS THEMA CYBERSECURITY ZU SCHAFFEN. NUR SO KANN IM ERNSTFALL SCHNELL REAGIERT WERDEN. DAS RISIKO FÜR FOLGESCHÄDEN IST GERINGER."

ULRICH IRNICH
CIO UND GLOBAL HEAD OF MODERNISATION
BEI VODAFONE DEUTSCHLAND

Takeaways IT-Security

1. AWARENESS SCHAFFEN

Da der Mensch das häufigste Einfallstor für Cyberattacken ist, sind regelmäßiges Training und Schulungen unverzichtbar, um die Mitarbeiter:innen für typische Angriffsmethoden zu sensibilisieren. Auch wenn solche Maßnahmen keinen absoluten Schutz bieten, sind sie eine wichtige Verteidigungslinie.

2. SCHWACHSTELLEN TESTEN

„Vulnerability Assessments“ sowohl in der internen Netzwerkumgebung des Unternehmens als auch über öffentliche Schnittstellen sollten alle Live-Systeme auf Schwachstellen untersuchen. Auf den Ergebnissen solcher Tests basiert dann der Auf- und Ausbau geeigneter Schutzlösungen.

3. FEHLERKULTUR GESTALTEN

Wer versehentlich einen IT-Vorfall verursacht, sollte sich nicht vor Konsequenzen fürchten müssen. Denn dies führt dazu, dass solche Fehler vertuscht werden und Angriffe länger unentdeckt bleiben. Eine konstruktive Fehlerkultur im Unternehmen ist aus vielen Gründen wichtig – Cybersicherheit gehört dazu.

4. PROAKTIVES SICHERHEITS-MANAGEMENT

Echtzeit-Security-Monitoring sollte rund um die Uhr sicherstellen, dass Cyberangriffe schnellstmöglich erkannt und abgewehrt werden können – also im Idealfall, bevor es zu spät ist. Ein proaktives Sicherheitsmanagement ist die Basis dafür.

5. KEIN BACKUP – KEIN MITLEID

Dieser geflügelte Spruch aus der IT-Sicherheit macht deutlich: Sicherheitskopien aller relevanten Daten und Systeme sind die wichtigste Basis für eine schnelle und erfolgreiche Wiederherstellung. Im Detail müssen die Konzepte dafür sicherstellen, dass eine Ransomware die Backups nicht gleich mitverschlüsseln kann.

6. RECOVERY-PLAN

Bei einem Cyberangriff ist es wichtig, schnell zu erkennen, woher die Angreifer:innen kommen, wo sich Schadsoftware versteckt und wie sie zuverlässig entfernt werden kann. Dafür müssen vorab definierte Prozesse vorhanden sein, die neben der Wiederherstellung der Daten helfen, das Problem zu lösen.

7. LÖSUNGSORIENTIERTE BERATUNG HOLEN

Cybersicherheit erfordert umfassende ineinandergreifende Lösungen. Das Vodafone-Lösungsportfolio für Cyber-Security bietet alle dazu nötigen Bausteine an – für alle Unternehmensgrößen und alle Phasen von Prävention über Detektion bis Reaktion.

Weitere Informationen finden Sie hier.

Lust auf mehr?

Spannender Content zum Thema IT-Sicherheit

Was hat **Stefan Stelling** aus dem Cyberangriff auf das Entsorgungsunternehmen Otto Dörner gelernt? Hören Sie hier in den Podcast.

Im Podcast mit **Stefan Würtemberger** von Marabu erfahren Sie hier mehr darüber, warum Cyber-Security kein IT-Thema ist.

Wie können Unternehmen mit der wachsenden Bedrohung durch Cyberangriffe umgehen und sich effektiv schützen? Genau dieser Frage geht **Patric Spethmann** als COO bei Marc O'Polo nach. Hören Sie hier in den Pocast.

Das Whitepaper liefert hier detaillierte Infos über mögliche **Schutzkonzepte** für Ihr Unternehmen.

Das Vodafone Enterprise Plenum liefert spannende Tech-Insights zu aktuellen **Business-Trends**. Mehr Infos finden Sie hier.