CYBER IM FOKUS

Unsichtbares Millionenrisiko

Wie kann sich die deutsche Wirtschaft vor Hackerangriffen schützen?

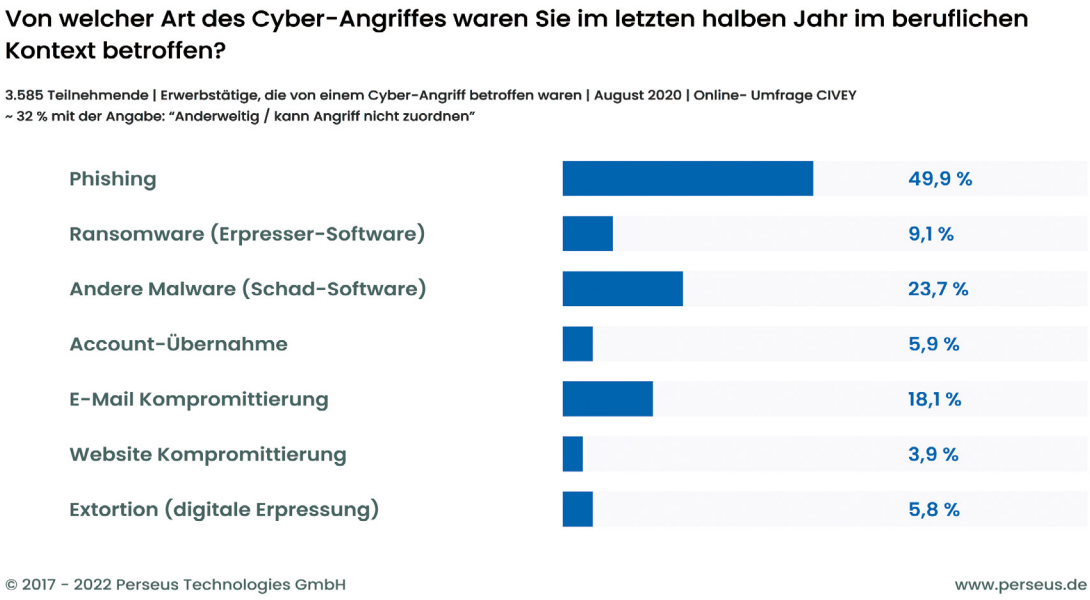
Von Kevin Püster

Cyberangriffe haben sich in den letzten Jahren zu einem der größten Geschäftsrisiken für die deutsche Wirtschaft entwickelt. Der finanzielle Schaden, der im Zuge eines Cyberangriffs entsteht, beläuft sich durchschnittlich auf 50.000 Euro (Hiscox Cyber Readiness Report 2020). Reputationsschäden, Vertragsstrafen oder mögliche Bußgelder, die aufgrund von Datenschutzverletzungen anfallen könnten, sind in dieser Summe oftmals noch nicht inbegriffen. Um sich vor Cyberangriffen zu schützen, müssen Unternehmen Cyberrisiken zunächst einmal erkennen und einschätzen können. Nur ein hohes Risikobewusstsein führt dazu, dass entsprechende Schutzmaßnahmen ergriffen werden. Im zweiten Schritt ist es wichtig, dass das Thema Cybersicherheit fest in der Unternehmensstruktur verankert wird. Und das beginnt an der Spitze des Unternehmens: Cybersicherheit muss Chefsache sein. Nur wenn das Top-Management die Bedeutung einer nachhaltigen Cybersicherheitsstrategie versteht und diese den Mitarbeitenden kommuniziert bzw. vorlebt, können Cyberrisiken innerhalb der Organisation reduziert und Cyberangriffe vermieden werden.

VIER DIMENSIONEN DER CYBERSICHERHEIT

Ein wichtiger Hinweis gleich vorneweg: Eine Einheitslösung gibt es nicht. Um sich nachhaltig gegen Bedrohungen schützen zu können, spielen verschiedene Faktoren zusammen: die vier Dimensionen der Cybersicherheit, bestehend aus der Technik, den Mitarbeitenden, dem Notfallmanagement und einer finanziellen Absicherung gegen das Restrisiko. Die Basis setzen die technischen Elemente wie zum Beispiel eine stets aktuelle Antiviren-Software oder eine aktive Firewall. Ohne sie hat ein Unternehmen heutzutage keine Chance, Cyberangriffe erfolgreich abzuwehren. Doch diese Maßnahmen reichen allein nicht aus. Zusätzlich müssen die Mitarbeitenden aktiv in die Cybersicherheitsstrategie eingebunden werden – sie gelten nach wie vor als Einstiegstor Nummer 1. Unüberlegte Klicks auf Links oder der falsche Download eines Dokuments reichen oftmals aus, um komplette Systeme und Netzwerke mit Schadsoftware zu infiltrieren und lahmzulegen. Aus einer durch uns durchgeführten Umfrage aus dem Jahr 2020 geht hervor, dass vor allem Phishing-Angriffe (50%) die Ursache von IT-Sicherheitsvorfällen waren. Durch mitarbeiterzentrierte Awareness-Schulungen wird die Belegschaft eines Unternehmens für Angriffsmuster sensibilisiert und potenzielle Angriffsversuche können schneller erkannt werden. Ähnlich wichtig ist die Vorbereitung auf den Ernstfall, denn eine 100-prozentige Sicherheit gibt es nicht. Sollte es zum Cybervorfall kommen, handelt es sich oftmals um Minuten, die darüber entscheiden, welches Ausmaß ein Cyberangriff annimmt. Mithilfe von Notfallplänen und regelmäßigen Übungen wird sichergestellt, dass Mitarbeitende schnell und richtig reagieren. Abgerundet wird die ideale Cybersicherheitsstrategie mit der finanziellen Absicherung durch eine Cyberversicherung. Da man heutzutage davon ausgehen muss, Opfer eines Cyberangriffs zu werden – egal wie groß oder klein das Unternehmen ist – empfiehlt sich der Abschluss einer solchen. Es gilt allerdings zu beachten, dass eine Cyber-Police nur ein Teil der Gesamtlösung ist, wenn auch ein sehr wichtiger.

Doch viele Unternehmen unterschätzen noch immer das Risikopotenzial, das von Cyberkriminellen ausgeht. Im April 2020 veröffentlichte der Gesamtverband der Deutschen Versicherungswirtschaft (GDV) eine Studie, die zeigt, dass 70 Prozent der befragten kleinen und mittleren Unternehmen das Risiko von Cyberkriminalität als sehr hoch einschätzen. Allerdings sehen nur 28 Prozent tatsächlich ein Risiko für das eigene Unternehmen. Die Gründe: Die von dem Unternehmen verarbeiteten Daten seien irrelevant (70%), das Unternehmen sei zu klein, um für Cyberkriminelle interessant zu sein (60%) oder die Systeme seien ausreichend geschützt (81%). Ein gefährlicher Irrglaube, denn für Cyberkriminelle ist jedes Unternehmen mit einer Internetanbindung ein potenzielles Ziel. Dabei variieren Cyberkriminelle in ihrem Vorgehen zwischen gezielten Angriffen auf bestimmte Un-



ternehmen und dem so genannten „Gießkannenprinzip": Hier werden Sicherheitslücken im großen Stil ausgenutzt oder Angriffswellen großflächig gestartet. Es kann also jeden treffen. Aktuelle Umfragezahlen des Bitkom belegen dies. 2020/2021 wurden neun von zehn Unternehmen Opfer von Datendiebstahl, Sabotage oder Spionage.

Neben immer dynamischeren und flexibleren Angriffen hat auch der Umzug ins Homeoffice die Unternehmen in den letzten Monaten vor große Herausforderungen gestellt. Viele mussten sehr schnell ihre IT-Infrastruktur verändern, um Kollaboration auf Distanz zu ermöglichen. Die Gefahrenquellen haben dadurch zugenommen: Ungesicherte Internetverbindungen, fehlende Firewalls, nicht installierte Sicherheitsupdates für Programme und Betriebssysteme sowie der Zugriff auf Firmenserver über private Laptops und Computer sind nur einige der potenziellen Schwachstellen, die Cyberkriminelle nutzen, um an sensible und vertrauliche Unternehmensdaten zu gelangen. Die fortschreitende Digitalisierung hat massive Auswirkungen auf die Cybersicherheitsstrategien von Unternehmen. Die IT-Infrastruktur wird mit jedem zusätzlichen Nutzer, jeder zusätzlichen Nutzerin und jeder neuen Anwendung komplexer. Jeder Einsatz von neuer Hard- und Software muss berücksichtigt und in das Sicherheitskonzept einbezogen werden. Die IT-Sicherheit der digitalen Infrastruktur muss daher konstant auf den Prüfstand gestellt werden.

In den letzten Jahren stieg die Nachfrage nach Cyberversicherungen. Gerade die Anzahl der mittelständischen Unternehmen mit einem Umsatz zwischen 10 und 50 Millionen Euro, die eine Cyberversicherung abgeschlossen haben oder zumindest darüber nachdenken, hat sich innerhalb von zwei Jahren verdoppelt (GDV). Die deutsche Wirtschaft erlitt allein in den Jahren 2020/2021 einen Gesamtschaden von 223 Milliarden Euro. Um diese finanziellen Risiken zu mindern, ist es essenziell, in den finanziellen Schutz vor Cyberrisiken zu investieren. Gleichzeitig ist es für die Versicherungswirtschaft herausfordernd, das komplexe Risikoprofil von Cyberrisiken so abzusichern, dass auch bei großen Angriffswellen eine Versicherbarkeit besteht.

Über die Versicherungswirtschaft hinaus besteht die Notwendigkeit, Cybersicherheit aktiver im Rahmen von regulatorischen und politischen Instrumenten zu verankern, um die Privatwirtschaft zu unterstützen. Zum Beispiel durch die Förderung von Forschung und Entwicklung oder durch die Erleichterung von Investitionen. Ebenfalls ist es wichtig, das generelle Bewusstsein zum Thema in der Bevölkerung zu schärfen. Ein weiterer Aspekt ist die Fokussierung auf zukünftige Talente und Experten. Ein Förderprogramm sowie Investitionen in die Aus- und Weiterbildung in den relevanten Sektoren und Bereichen stellen nachhaltig sicher, dass auch die Cyberrisiken von morgen bekämpft werden. Hier steht u.a. die Politik in der Verantwortung.

Kevin Püster, Geschäftsführer
Perseus Technologies GmbH