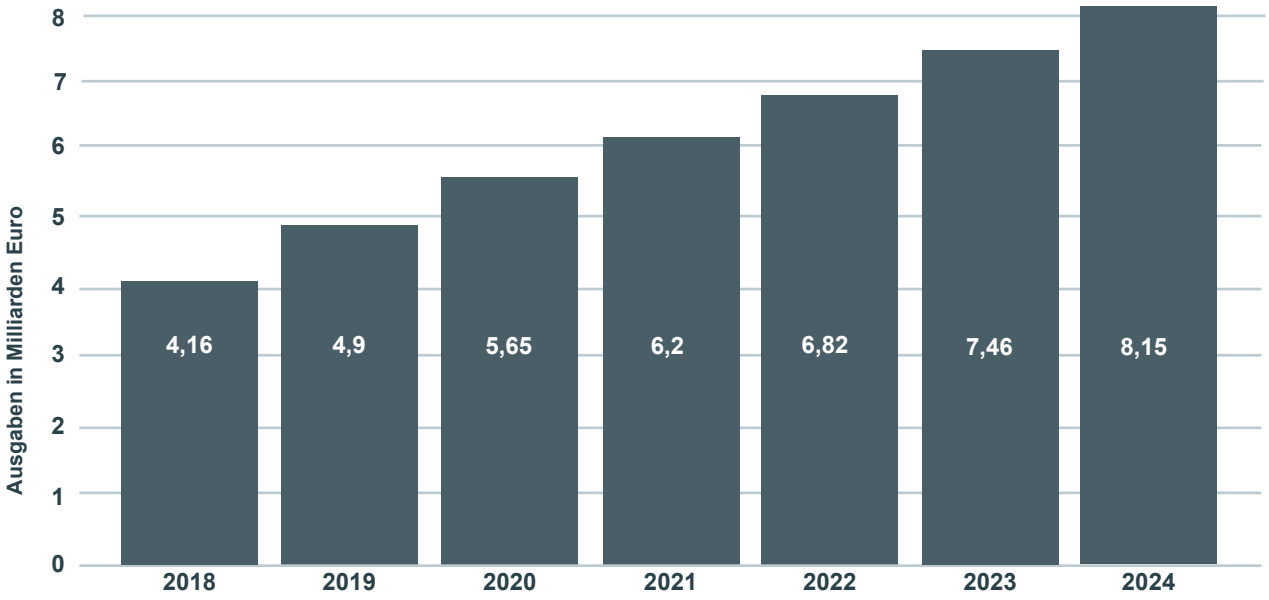
Cyber Security als **zentraler Erfolgsfaktor** für Unternehmen

Aktuelle Bedrohungen und Tipps zur Erarbeitung
einer erfolgreichen Cyber-Security-Strategie

claranet cyber security

Cyber Security als zentraler Erfolgsfaktor für Unternehmen

In Zeiten von Industrie 4.0, Digitalisierung und Cloud-Anwendungen nimmt die IT-Abhängigkeit von Unternehmen branchenübergreifend stetig zu. Kaum ein Unternehmen kommt heute noch ohne eine professionelle IT-Infrastruktur mit Zugang zum Internet aus. Gleichzeitig werden gezielte Angriffe auf IT-Infrastrukturen immer professioneller und komplexer – das Schadenspotenzial für betroffene Unternehmen steigt dadurch stetig an. Neben dem massiven Imageschaden durch Datenklau fürchten Unternehmen aber auch Umsatzeinbußen und Bußgelder von Datenschutzbehörden. Allein im letzten Jahr hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) rund 144 Millionen neue Schadprogramm-Varianten[1] identifiziert und über 40.000 Bot-Infektionen pro Tag beobachtet.[2] Die Unternehmen versuchen, sich gegen die Bedrohung zu schützen, und investierten jedes Jahr mehr Geld in die IT-Sicherheit: Waren es im Jahr 2019 noch etwa 4,9 Milliarden Euro, so werden sich die Ausgaben im Jahr 2024 voraussichtlich auf etwa 8,15 Milliarden Euro belaufen.



Ausgaben für IT-Sicherheit in Deutschland von 2018 bis 2020. Prognose von 2021 bis 2024
(Quelle: https://de.statista.com/statistik/daten/studie/1041736/umfrage/ausgaben-fuer-it-security-in-deutschland/)

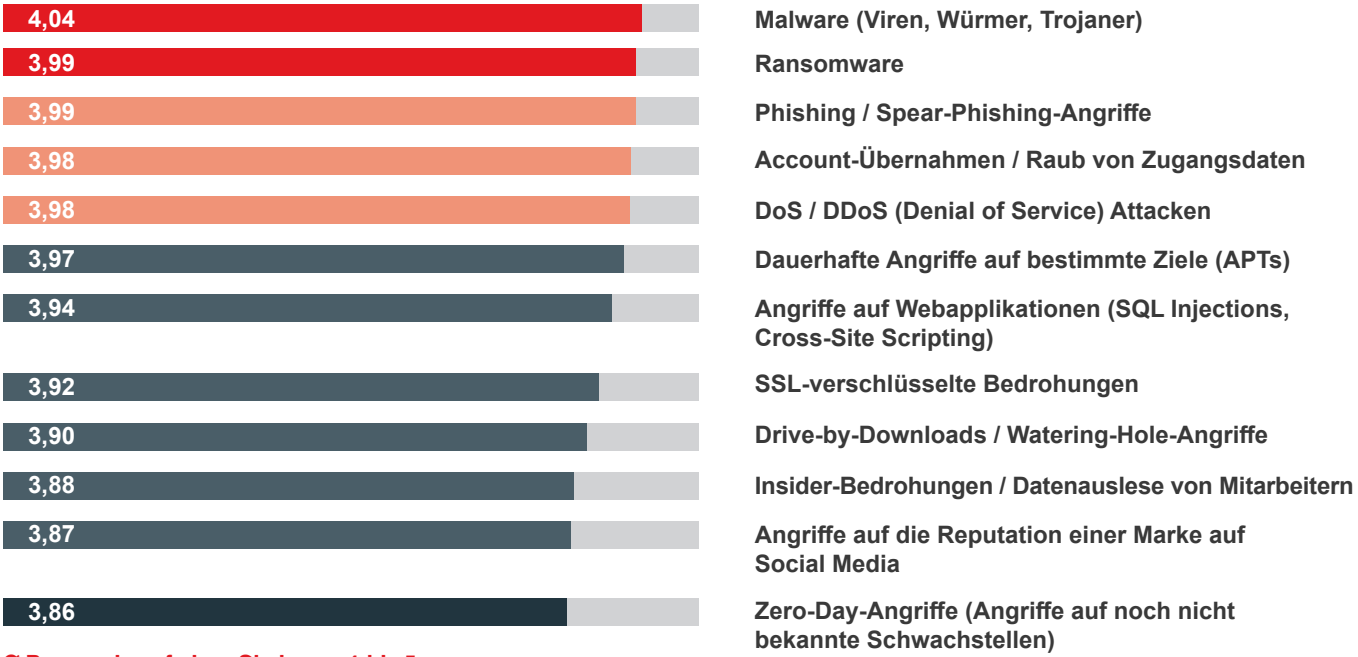
1 und 2 https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html

Wichtiger als die Frage nach der Höhe der Ausgaben ist jedoch die richtige Strategie im Umgang mit dem Thema Cyber Security. In diesem Whitepaper gehen wir daher auf die konkreten Bedrohungen durch Cyberattacken ein und zeigen anhand einer strukturierten Checkliste auf, wie Sie als Verantwortlicher für die IT-Sicherheit Ihres Unternehmens eine erfolgreiche Strategie gegen Cyberattacken erarbeiten. Wir stellen die Bedeutung von Penetration-Testing- und Continuous-Security-Testing-Methoden heraus und erklären, warum das Security Awareness Training für eine nachhaltige IT-Sicherheit so wichtig ist.

Aktuelle Bedrohungen durch Cyberattacken

Die Schäden für die deutsche Wirtschaft sind enorm: Einer Studie des Digitalverbands Bitkom zufolge verursachten Cyberattacken im Jahr 2021 einen Gesamtschaden von 223 Milliarden Euro für Unternehmen in Deutschland. Analoge und digitale Angriffe durch Sabotage, Datendiebstahl und Spionage haben damit einen fast doppelt so hohen Schaden verursacht wie noch vor zwei Jahren.[3] Auch der Anteil der betroffenen Unternehmen unterstreicht die besorgniserregende Entwicklung: Waren in den Jahren 2018/2019 etwa 75 Prozent der Unternehmen Opfer eines Cyberangriffs, so beläuft sich der Anteil in den Jahren 2020/2021 schon auf 88 Prozent.[4] Cyberattacke ist nicht gleich Cyberattacke. Auf die Frage, welche Art von Cyberattacken als besonders bedrohlich wahrgenommen werden, nannten die in einer Cyber-Edge-Studie befragten IT-Entscheidungsträger vor allem Malware- und Phishing-Attacken sowie Ransomware- und Account-Takeover-Angriffe.

Jedes zehnte Unternehmen in Deutschland sieht aktuell seine geschäftliche Existenz durch Cyberattacken bedroht.[5]



Welche Cyberattacken werden als besonders bedrohlich wahrgenommen?
(Quelle: https://cyber-edge.com/wp-content/uploads/2021/04/CyberEdge-2021-CDR-Report-v1.1-1.pdf)

3-5 https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-als-220-Milliarden-Euro-Schaden-pro-Jahr

Schritt für Schritt zur Cyber Security – Tipps für eine erfolgreiche Strategie

Die Zahlen zeigen, dass das Thema IT-Sicherheit in den Chefetagen der Unternehmen angekommen ist. Bei der Umsetzung in die Praxis stehen viele jedoch vor großen Herausforderungen. Neben dem notwendigen Fachwissen fehlt es häufig an einer lückenlosen Sicherheitsstrategie als Grundlage für geeignete IT-Sicherheitsmaßnahmen.

Mit unserer Checkliste zum Thema Cyber Security können Sie Schritt für Schritt eine erfolgreiche Strategie zur Abwehr von Cyberbedrohungen entwickeln:

1. Transparenz schaffen
Die Voraussetzung für eine erfolgreiche Strategie zur Abwehr von Cyberangriffen ist ein tiefgreifendes Verständnis von den IT-Prozessen im eigenen Unternehmen. Im ersten Schritt geht es daher primär darum, umfassende Einblicke in alle Prozesse zu gewinnen – vom Netzwerk über die Cloud bis zum Endpunkt. Welche mobilen Endgeräte stellen eine Verbindung zu welchem Netzwerk her, welche Computer arbeiten mit welchen Betriebssystemen, und welche Benutzer sind welchen potenziellen Bedrohungen ausgesetzt? Diese Fragen gilt es, transparent zu beantworten.

2. Verantwortlichkeiten klären
Angesichts immer komplexerer Bedrohungen durch Cyberangriffe ist eine gut funktionierende IT-Abteilung heutzutage eine Grundvoraussetzung für den nachhaltigen Unternehmenserfolg. Dabei sind vor allem die IT-Governance und die IT-Steuerung von großer Bedeutung. Die IT-Governance beschreibt die Organisation, Steuerung und Kontrolle der IT zur optimalen Unterstützung der Unternehmensziele – sie umfasst neben der Ernennung eines CIOs und IT-Managers auch das Aufstellen einer Sicherheits-organisation und die Etablierung geeigneter Steuerungs- und Kontrollmechanismen.

3. Schutzmaßnahmen definieren
Der präventive Schutz kritischer Systeme und Funktionen zählt traditionell zu den Kernaufgaben der IT-Abteilung und umfasst Bereiche wie Access Management, Perimetersicherheit,

Endpoint-Sicherheit, Systemhärtung und -wartung sowie Datensicherheit. Um trotz hoher Sicherheitsanforderungen agil zu bleiben, folgen immer mehr Unternehmen dem DevSecOps-Gedanken: Software-Entwicklung, IT-Sicherheit und IT-Betrieb rücken zusammen, um mit neuen Prozessen und Tools für Entwicklungsgeschwindigkeit, Qualität und Sicherheit zu sorgen.

4. Bedrohungen sichtbar machen und priorisieren

Die eigenen IT-Schwachstellen mit den professionellen Methoden krimineller Hacker erkennen – das Penetration Testing liefert die notwendige Transparenz, um Bedrohungen zu erkennen und Verbesserungen vorzunehmen. Beim Penetration Testing kommt es darauf an, eine passende Simulationsart für den Angriff auf die eigenen Systeme zu wählen und die richtigen Ziele zu identifizieren. Auf diese Weise gelingt es, Schwachstellen frühzeitig zu erkennen und das Risiko für Cyberangriffe zu bewerten. Auf Grundlage dieser Einschätzung können geeignete Maßnahmen erarbeitet und die Schwachstelle zukunftssicher ausgebessert werden. Um die IT-Sicherheit langfristig zu gewährleisten, sollten Unternehmen gezielte Penetration-Tests mit kontinuierlichen Sicherheitsüberprüfungen begleiten. Während klassische Penetration-Tests immer nur einen bestimmten Augenblick erfassen, dient das Continuous Security Testing der kontinuierlichen Überprüfung der IT-Sicherheitsperformance. Regelmäßige manuelle Penetration-Tests werden kombiniert mit automatisierten Sicherheits-Checks.

5. Mitarbeiter gezielt schulen

Cyber Security geht alle an – vom Kaufmann in der Buchhaltung über den Konstruktionsingenieur bis hin zum CEO. Professionelle Hacker versuchen Mitarbeiter heutzutage gezielt mit Social-Engineering-Methoden zu täuschen, um Zugang zu Netzwerken zu erlangen. Die Cyber Security muss daher ein fester Bestandteil der täglichen Arbeit werden. Dabei geht es nicht nur um das regelmäßige Ändern von Passwörtern, sondern vielmehr um ein wachsames Auge im Umgang mit Cyberbedrohungen. Durch Security Awareness Trainings können Unternehmen ihre Belegschaft gezielt auf die Abwehr von Phishing-Attacken und anderen Social-Engineering-Methoden vorbereiten.

6. Für den Ernstfall wappnen

Im Fall einer erfolgreichen Attacke ist es wichtig, schnell und besonnen zu reagieren, um mögliche Auswirkungen einzudämmen. Neben der Wiederherstellung der betroffenen Systeme und Daten sind die interne und externe Kommunikation wichtig. Damit alle Beteiligten im Ernstfall richtig reagieren, sollten Response- und Recovery-Maßnahmen sorgfältig geplant und trainiert werden.

Diese Checkliste bietet Ihnen eine Grundlage, um das Thema Cyber Security im Unternehmen strategisch anzugehen und die Voraussetzungen für eine wirkungsvolle und effektive Verteidigung gegen Cyberangriffe zu schaffen. Abhängig davon, wo Sie aktuell stehen, werden manche Punkte mehr, manche weniger Aufwand für Sie bedeuten. Manche sind Teil eines langfristigen Prozesses, andere lassen sich kurzfristig umsetzen. Im Folgenden möchten wir Ihnen drei ausgewählte Methoden vorstellen, mit denen Sie direkt starten können, um Schwachstellen zu erkennen und das Sicherheitsniveau Ihres Unternehmens zu verbessern.

Methoden zum Aufdecken, Beseitigen und Vermeiden von Schwachstellen

Mit Penetration Testing Schwachstellen gezielt aufdecken und beseitigen

Penetration-Tests verfolgen das Ziel, Unternehmen vor schwerwiegenden Sicherheitslücken und daraus resultierenden Angriffen durch professionelle Hacker zu schützen. Grundlage der sogenannten „Pentests“ ist die Simulation gezielter, realistischer Angriffe auf die sicherheitsrelevanten IT-Systeme des eigenen Unternehmens.

Die Herausforderung bei der Durchführung professioneller Penetration-Tests liegt darin, sich in die Perspektive eines Angreifers zu versetzen, potenziell interessante Angriffsflächen zu erkennen und gefundene Schwachstellen zu analysieren: Wie hoch sind das Angriffsrisiko und potenzielle Schäden einzuschätzen? Und welche Priorisierung ist beim Beheben der gefundenen Lücken sinnvoll?

Dass Penetration-Tests auch in vielen deutschen Unternehmen eine wichtige Rolle spielen, zeigt eine teleResearch-Statistik[6] aus dem Jahr 2021: 55 Prozent der Befragten haben in den letzten zwei Jahren in Penetration-Tests investiert und diese Maßnahme zur Erfassung potenzieller Schwachstellen eingesetzt. Allerdings zeigt die Statistik auch, dass die Methode kein Allheilmittel ist. Vielmehr sollte sie Teil einer ganzheitlichen Sicherheitsstrategie sein, in der das Sicherheitsniveau eines Unternehmens kontinuierlich verbessert wird.

Risiken automatisch erkennen: durch Continuous Security Testing

Während Penetration-Tests jeweils nur eine Momentaufnahme des aktuellen Zustandes der IT-Security sind, gewährleistet Continuous Security Testing eine fortlaufende Überprüfung von IT-Infrastruktur und Applikationen auf Schwachstellen und Sicherheitslücken. Das ist vor allem in Hinblick auf die ständige Weiterentwicklung und Veränderung von Applikationen wichtig, durch die sich das Gefährdungspotential für Cyberangriffe sehr schnell ändern kann.

Continuous Security Testing kombiniert die Vorteile manueller Penetration-Tests mit parallel laufenden, kontinuierlichen Schwachstellenscans. Die gefundenen Schwachstellen werden von erfahrenen Penetration-Testern verifiziert und auf mögliche Auswirkungen und Geschäftsrisiken überprüft und bewertet. Darauf basierend werden dann detaillierte und präzise Alerts, Analysen und Empfehlungen erstellt.

Die Vorteile von Continuous-Security-Testing-Maßnahmen auf einen Blick:

- Unternehmen gewinnen schneller Erkenntnisse über IT-Schwachstellen,
- sie erfüllen Compliance-Anforderungen in Bezug auf regelmäßige Security Testings
- und es gelingt ihnen, einen Prozess zur kontinuierlichen Optimierung ihrer IT-Sicherheit zu etablieren.

6 https://de.statista.com/statistik/daten/studie/186758/umfrage/sicherheitsvorkehrungen-gegen-spionage-und-datenklau-in-deutschen-unternehmen/

Mit Security Awareness Training stets auf dem neusten Stand bleiben

Der „Human Factor Report 2021“ von Proofpoint[7] zeigt eindrucksvoll auf, dass Cyberkriminelle es vor allem auf Menschen und weniger auf die IT-Systeme selbst absehen: Mehr als 99 Prozent aller beobachteten Cyberangriffe erfordern eine menschliche Interaktion und sind somit dem Social Engineering zuzurechnen. Ob durch betrügerische E-Mails oder durch das Stehlen von Zugangsdaten – häufig steht nur der Mitarbeiter zwischen dem Hacker und dem Zugang zum IT-System. Die beste Firewall ist nutzlos, wenn Cyberkriminelle über unachtsame Mitarbeiter Zugang ins System erlangen.

Zu den typischen Social-Engineering-Methoden gehören beispielsweise das massenhafte Verschicken gefälschter E-Mails (Phishing) sowie das Ködern von Mitarbeitern durch das Verschenken infizierter USB-Sticks (Baiting). Auch das sogenannte Tailgating, das physische Eindringen eines Angreifers in geschlossene Unternehmensbereiche, hat zugenommen.

Mit Security Awareness Trainings bereiten Unternehmen ihre Mitarbeiter gezielt auf Social-Engineering-Methoden vor und sensibilisieren sie für IT-Angriffe von außen. Im Rahmen regelmäßiger Schulungen geht es darum, die Belegschaft mit praxisnahen Beispielen über reale Gefahren zu informieren und Handlungsempfehlungen für den Umgang mit Social-Engineering-Methoden zu vermitteln. Der Erfolg spricht für sich: Einer Umfrage im „Security Awareness Training Report“ zufolge konnte die Erfolgsrate von Phishing und Malware durch simulierte Übungsattacken im Zuge von Security Awareness Trainings von 40 bis 50 Prozent auf null bis fünf Prozent reduziert werden.[8]

7 https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-human-factor-report.pdf
8 https://www.knowbe4.com/hubfs/SecurityAwarenessTrainingDeploymentsDeterDefeatHackers.pdf

Fazit

Bei der Erarbeitung einer Verteidigungsstrategie kommt es auf ein ganzheitliches Security-Gesamtkonzept an, das IT-technische Maßnahmen mit gezielten Mitarbeitertrainings kombiniert und speziell auf die Unternehmenssituation zugeschnitten ist. Dabei zeigt sich, dass eine Kombination aus gezielten Penetration-Tests, systematisiertem Continuous Security Testing und regelmäßigen Security Awareness Trainings im ersten Schritt besonders vielversprechend ist.

Die Key Takeaways im Überblick:

- **Cyberangriffe** verursachen jedes Jahr einen Schaden von mehr als 100 Milliarden Euro in der deutschen Wirtschaft – Tendenz steigend.
- Mithilfe unserer **Checkliste** gelingt es Ihnen, sich strategisch auf die Neuausrichtung Ihrer IT-Systeme vorzubereiten.
- **Penetration Testing & Continuous Security Testing** helfen Ihnen dabei, Sicherheitslücken gezielt aufzudecken, einzuschätzen und zu beseitigen. Sie können und wollen jedoch keine Garantie gegen Angriffe bieten.
- Cyberangriffe erfordern in vielen Fällen eine menschliche Interaktion – **daher nehmen Hacker die Mitarbeiter ins Visier.** Mit Security Awareness Trainings gelingt es Ihnen, die Anfälligkeit Ihres Unternehmens gegenüber Cyberangriffen signifikant zu reduzieren.
- **Sicherheitsstrategien** entfalten nur dann ihre volle Wirkung, wenn sie tief in der Organisationsstruktur und Arbeitskultur eines Unternehmens verankert sind und gelebt werden.

Unternehmen setzen bei der Ausarbeitung von Strategien und der Durchführung konkreter Maßnahmen immer häufiger auf die Zusammenarbeit mit erfahrenen Cybersicherheitsexperten. So sieht Claranet bereits seit einigen Jahren einen wachsenden Bedarf an Security Services bei deutschen Unternehmen. Unser Cyber Security Portfolio orientiert sich am NIST Cybersecurity Framework (siehe Abbildung) und umfasst neben Penetration-Testing-Maßnahmen auch Continuous Security Testings und Security Awareness Trainings, die den Funktionsbereichen „Protect“ und „Detect“ zugeordnet werden.

Funktionsbereiche des NIST Cybersecurity Frameworks
(Quelle: https://www.nist.gov/cyberframework)

Kontakt

Sie möchten sich genauer über das Thema
Cyber Security informieren?
Schreiben Sie uns: **cybersecurity@claranet.de**

claranet cyber security