Spielen Sie Russisch Roulette mit der Zukunft Ihres Unternehmens?

Wie Angreifer an Ihre sensiblen Daten kommen und Sie Ihre IT-Infrastruktur schützen

Hacker, Cyberkriminalität und Wirtschaftsspionage: Die Anzahl und Komplexität von Angriffen auf Unternehmen nimmt stetig zu und verfolgt das Ziel, wichtige Daten und Informationen zu stehlen, sabotieren und manipulieren.

Mittelständische Unternehmen rücken vermehrt in das Visier der Cyberkriminellen, da hier wertvolle Betriebs- und Geschäftsgeheimnisse liegen und Informationen oftmals nur unzureichend gesichert sind. Ist ein Angriff erstmal geglückt, sind die Folgen enorm: finanzielle Verluste, Reputationsschäden und verlorenes Kundenvertrauen drohen.

In unserem Whitepaper erklären wir, wie Angreifer an Ihre sensiblen Daten gelangen können und geben Ihnen ein Grundverständnis für ein wirksames Sicherheitsmanagement.

Es wird ein Modell, die Cyber Kill Chain, aufgezeigt, mit dem das Vorgehen der Täter phasenweise erklärt wird. Dies gibt einen Überblick über die einzelnen Handlungsschritte und bietet Ihnen eine Grundlage, Ihre IT-Sicherheit dementsprechend zu überprüfen und Attacken wirksam abzuwehren. Darauf aufbauend erfahren Sie, wie eine Sicherheitsstrategie aussehen kann und was Sie bei der Auswahl von entsprechender Software beachten sollten.

Inhalt

Zielscheibe Mittelstand: Anzahl der Cyberangriffe steigt auf Rekordniveau

Würden Sie Russisch Roulette spielen? Höchst wahrscheinlich nicht. Das Risiko ist viel zu hoch. Und dennoch: fast täglich spielen es Unternehmen in digitaler Form durch eine unzureichende IT-Sicherheitsstrategie und setzen dabei die Zukunft ihres Unternehmens und ihrer Mitarbeiter aufs Spiel.

Für das aktuelle Jahr stellt der *2018 Cyber Threat Report* des Sicherheitsspezialisten SonicWall bereits eine Rekordzahl an Bedrohungen fest.[1] Die Bandbreite reicht von Ransom- und Malware, über verschlüsselte Angriffe bis hin zu chipbasierten Bedrohungen. Seit Beginn des Jahres wurden allein 181,5 Millionen Ransomware- und 5,99 Milliarden Malware-Angriffe verzeichnet.[2] Für Bill Conner, CEO von SonicWall ist eins klar: „Das Cyber-Wettrüsten entwickelt sich schneller als je zuvor – mit drastischen Konsequenzen für Unternehmen, Regierungsbehörden, Bildungs- und Finanzinstitutionen und Organisationen in vielen anderen Branchen".[3] Auch das Bundesamt für Sicherheit in der Informationstechnik betont fest, dass die Risiken durch Cyberangriffe zunehmen[4].

Die finanziellen Folgen von solchen Angriffen sind erheblich. Allein im letzten Jahr haben Cyberangriffe Schäden in Höhe von 56 Milliarden Euro bei deutschen Unternehmen verursacht[5]. Die Kosten sind allerdings nicht das einzige Problem. 51% der betroffenen Unternehmen klagen über Produktions- und Betriebsausfälle und auch Reputationsschäden (16,5%) bleiben nicht aus.[6]

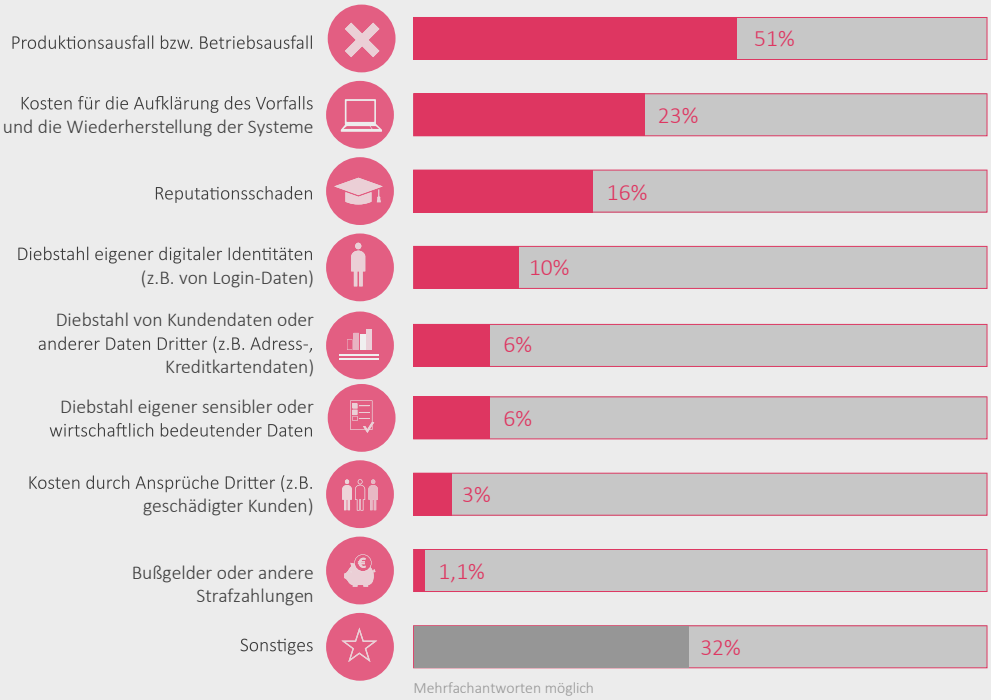
Cyberangriffe sind gezielte Maßnahmen, die sich gegen die Infrastrukturen der IT richten und dienen der Informationsbeschaffung, Sabotage oder Manipulation von Daten.

Ransomware sind Schadprogramme, die den Zugriff auf Systeme und Daten entweder einschränken oder ganz unterbinden. Für die Wiederherstellung des vollständigen Zugriffs wird dann ein Lösegeld verlangt.

Bei **Malware** handelt es sich um schädliche Software, die gezielt eingesetzt wird, um Schaden anzurichten. Dieser kann aus einem Verlust sensibler Daten oder auch der Schädigung der IT-Systeme bestehen.

Art der Schäden durch Cyberangriffe[7]

Anteile in % an allen Befragten



Mehrfachantworten möglich

Trotz dieser steigenden Gefahr vernachlässigen viele Unternehmen die Sicherheit der eigenen IT.[8] Das ist ein Spiel mit der Zukunft des Unternehmens und es ist nur eine Frage der Zeit, bis bestehende Sicherheitslücken von Kriminellen ausgenutzt werden. Laut einer Studie des Bundesamts für Sicherheit und Informationstechnik steigt das Bewusstsein in Unternehmen für die Bedrohung durch Cyberangriffe zwar an, aber die Umsetzung von entsprechenden Maßnahmen verläuft noch schleppend.[9]

Fakt ist, dass Angreifer keinen Unterschied zwischen Konzernen und Mittelstand machen. Viele mittelständische Unternehmen wiegen sich in der Sicherheit, dass ihr Bekanntheitsgrad möglicherweise nicht groß genug ist, um Opfer von Cyberangriffen zu werden. Hier liegt jedoch ein Trugschluss vor. Besonders auch in mittelständischen Unternehmen liegen viele wertvolle und schützenswerte Informationen wie Patente, Verträge, Kundendaten und finanzielle Informationen vor. Unternehmen digitalisieren zunehmend ihre Prozesse und vernetzen sich mit Geschäftspartnern, Lieferanten und Kunden. Somit entstehen komplexe Infrastrukturen, die auch eine neue Bewertung der Informationssicherheit fordern. Viele mittelständische Unternehmen investieren jedoch nicht die notwendigen Ressourcen und riskieren somit Opfer von Cyberangriffen zu werden.[10] Die Budgets der IT-Abteilungen sind für das letzte Jahr im Vergleich zu 2016 sogar um 6% geschrumpft.[11]

Cyberangriffe sind allerdings so vielschichtig, dass die Abwehr nur mit den richtigen technischen Lösungen und dem Know-how der Mitarbeiter funktionieren kann. Essentiell ist es, alle Mitarbeiter im richtigen Umgang mit Regeln und Richtlinien zur IT-Sicherheit im Unternehmen zu schulen. Ahnungslose Mitarbeiter stellen eine nicht zu unterschätzende Gefahrenquelle dar, wie eine aktuelle Studie von Kaspersky Lab festgestellt hat.[12] Die Sensibilisierung sollte bei Datenschutz und Internetsicherheit beginnen und auch Themen wie Identitätsmanagement, Cloud Security und die Sicherheit mobiler Endgeräte umfassen[13].

Die tägliche Realität ist, dass Angreifer nach dem Zugriff auf Systeme und Netzwerke ihrer Opfer wertvolle Informationen erlangen. So können sie beispielsweise Kunden- oder Personaldaten stehlen oder Zugriff auf Betriebsgeheimnisse erhalten.[14] Dadurch werden Datenschutzrichtlinien verletzt, das Vertrauen von Kunden missbraucht und es kann zu Unterbrechungen des Geschäftsbetriebs kommen. Ist der Super-GAU eingetroffen, herrscht Panik und Hektik. Doch dann ist es meistens schon zu spät. Unternehmen sehen sich mit Herausforderungen konfrontiert, die in der nötigen Zeit nicht zu lösen sind, denn Sicherheit ist kein Zustand, den man von jetzt auf gleich herstellen kann. Folglich dürfen sich Unternehmen nicht nur im Reaktionsmodus bewegen, sondern sie sollten in das aktive und präventive Handeln übergehen.

Anatomie eines Angriffs – die Cyber Kill Chain

Nutzen und Einsatz der Cyber Kill Chain

Cyberangriffe auf Ihr Unternehmen können Sie nur verhindern, wenn Sie das Vorgehen des Angreifers kennen und die potentiellen Angriffspunkte schützen.

Aufgrund dessen hat der US-amerikanische Rüstungs- und Technologiekonzern Lockheed Martin den Ablauf solcher Attacken modelliert.[15] Dieses Modell ist auf Malware-Attacken ausgerichtet, es hilft aber auch Advanced Persistent Threats (APT) abzubilden. Angriffe können damit analysiert werden, sodass eine gezielte Abwehr entlang der einzelnen Phasen möglich ist.

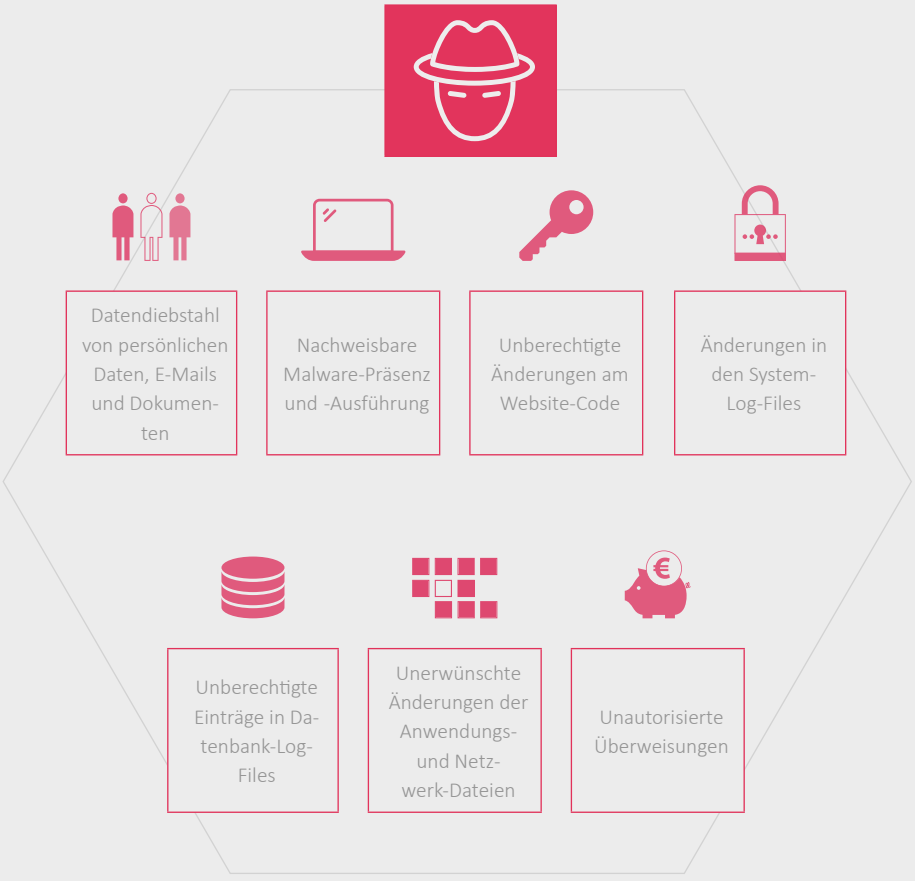
Unternehmen können ferner mit Hilfe der Cyber Kill Chain bereits vorhandene Sicherheitsmaßnahmen überprüfen und Software-Lösungen lassen sich anhand ihrer Funktionen den unterschiedlichen Phasen zuordnen. Dies ermöglicht, die eingesetzten Lösungen dahingehend zu überprüfen, ob sie einen Angriff abwehren können. Außerdem werden mögliche Lücken in der Abwehr frühzeitig erkannt.

Wird ein Angriff identifiziert, können wichtige Folgeschritte anhand der Phasen der Cyber Kill Chain abgeleitet werden. Hierbei sollten Unternehmen auch immer Technologien einsetzen, die ihnen Transparenz über ihre aktuelle Sicherheitslage verschaffen.[16]

Advanced Persistent Threats (APT) sind Zugriffe durch nicht autorisierte Personen auf ein Netzwerk mit dem Ziel dort lange unentdeckt zu bleiben und Daten zu stehlen.

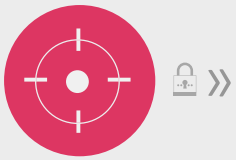
Wichtig zu wissen ist, dass ein externer Angreifer alle Phasen durchlaufen muss, um an Ihre sensiblen Daten und Informationen zu gelangen. Unternehmen können jedoch in jeder dieser Phasen die Attacke abwehren und somit die Cyber Kill Chain unterbrechen.[17] Außer Acht lassen sollte man dabei jedoch nicht, dass in jeder der Phasen bereits ein Schaden entstehen kann. Folglich ist es ratsam, auch die Abwehr mehrstufig aufzubauen, um so einen bestmöglichen Schutz sicherzustellen.

Mögliche Anzeichen, dass Ihr Unternehmen angegriffen wurde



Die Angriffs- und Verteidigungsstrategie der Cyber Kill Chain

Nachfolgend finden Sie den Ablauf der Cyber Kill Chain mit den Phasen, die der Angreifer durchlaufen muss und Möglichkeiten für Ihre Verteidigung.



Phase 1 | «Reconnaissance» – Identifizierung des Ziels

Angriffsstrategie

Zunächst sucht ein Angreifer nach einem Ziel und sammelt Informationen über dieses Unternehmen. Darunter fallen Daten, die mitunter auch einfach über öffentliche Quellen ausfindig zu machen sind, beispielsweise über die Firmenstruktur, E-Mail-Adressen von Mitarbeitern oder Pressemitteilungen.

Verteidigungsstrategie

In der Anfangsphase kann es sehr schwer zu erkennen sein, dass Ihr Unternehmen zu einem potentiellen Angriffsziel geworden ist. Achten Sie beispielsweise auf Besucher-Logs Ihrer Website, die auf verdächtige Suchanfragen hinweisen oder minimieren Sie die öffentlich verfügbaren Informationen.[18]

Phase 2 | «Weaponization» – Vorbereitung des Angriffs

Angriffsstrategie

Für die Durchführung des Angriffs werden passende Tools ausgewählt, die von dem gewählten Vorgehen und dem Ziel abhängig sind. Es handelt sich beispielsweise um Malware oder Ransomware.

Verteidigungsstrategie

Mit Hilfe spezieller Analyse-Tools ist es möglich, Angriffe aufzuspüren und die Auswirkung von Schadsoftware abzuschätzen.[19]

Mit Hilfe von **Advanced Threat Protection** können hochkomplexe Angriffe auf Netzwerk, Geräte und Daten entdeckt, untersucht und beseitigt werden.

Bei einem **Exploit** handelt es sich um Code, der Sicherheitslücken ausnutzt, um auf Server zuzugreifen oder Schadsoftware zu installieren. Die Art des Exploits ist vielfältig, oft genannt werden remote oder lokal ausgeführte Exploits, DoS-Exploits oder auch SQL-Injection-Exploits. Das heißt, Server können überlastet sein oder Datenbanken manipuliert.

Das **Intrusion Prevention System** erkennt Angriffe, informiert Administratoren über unregelmäßiges Verhalten und kann selbständig Maßnahmen zum Schutz ergreifen.

Phase 3 | «Delivery» – erste Schritte zur Durchführung des Angriffs

Angriffsstrategie

Im nächsten Schritt beginnt die Durchführung der Cyberattacke. Auf Basis der gesammelten Informationen wird ein Medium für den Angriff gewählt. Dieser kann entweder auf direktem Wege über die Webserver oder infizierte E-Mails, USB-Sticks, Social Media Interaktionen oder durch Phishing auf kompromittierten Websites vollzogen werden.

Verteidigungsstrategie

Diese Phase ist für die Verteidigung sehr entscheidend, um die Attacke zu blockieren. Überwachen Sie die möglichen Angriffswege zum Beispiel durch den Einsatz von Advanced Threat Protection Lösungen. Analysieren Sie auch bereits entdeckte Angriffe und untersuchen Sie Auswirkungen auf das System und Netzwerk, um die Ziele des Täters zu verstehen.[20]

Phase 4 | «Exploitation» – Aufspüren von Sicherheitslücken

Angriffsstrategie

Der Angreifer nutzt eine Sicherheitslücke im Zielsystem aus, wobei es sich um Software, Hardware oder Firmware handeln kann. Der Angreifer richtet seine Strategie auf die technische Kompromittierung dieser aus. Eine Sicherheitslücke können hier auch Mitarbeiter eines Unternehmens sein, die nicht ausreichend sensibilisiert sind und Opfer von Identitätsfälschungen werden.

Verteidigungsstrategie

Der Fokus sollte hier auf der Aufdeckung möglicher Angriffswege liegen: meist sind diese technik- oder personenbezogen. Es können Penetrationstests genutzt werden, um etwaige Schwachstellen aufzudecken. Verwenden Sie virtuelle LANs oder IPsec, um die Datenübertragung zu sichern. Schützen Sie sich vor Exploits, indem Sie veröffentlichte Updates oder Patches zeitnah installieren. Zudem sollten Intrusion Prevention Systeme (IPS) eingesetzt werden, die gegenüber herkömmlichen Firewalls einen zusätzlichen Schutz vor Angriffen auf Netzwerke oder Computersysteme bieten.

Phase 5 | «Installation» – Sicherstellung des beständigen Zugriffs

Angriffsstrategie

Nach dem Exploit wird Malware auf dem Zielsystem installiert und eine Backdoor errichtet. Diese umgeht den normalen Zugriffsschutz von Soft- oder Hardware und stellt den beständigen Zugriff auf das Zielsystem sicher.

Verteidigungsstrategie

Überprüfen Sie verdächtige Installationen, Aktivitäten, Signaturen und Zertifikate und schauen Sie, ob Berechtigungen bestehen, die so nicht erteilt wurden. Ziel ist es, die vom Täter bereits vollzogenen Maßnahmen zu unterbinden.[21]

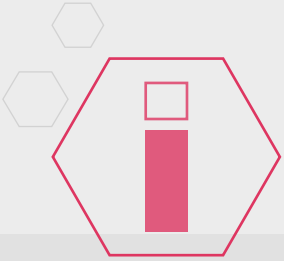
Phase 6 | «Command & Control» – Fernsteuerung des Zielsystems

Angriffsstrategie

Der Angreifer erhält durch die Malware die Information, dass die Attacke erfolgreich durchgeführt wurde. Der infizierte Computer beziehungsweise das Netzwerk kann über zentralisierte Befehle gesteuert werden, beispielsweise im Rahmen eines Botnets. Die Schadsoftware wird aus der Ferne gesteuert, um Daten zu exfiltrieren.

Verteidigungsstrategie

Nachdem die Angriffswege identifiziert sind, können abhängig davon Handlungsempfehlungen definiert und so die Schwachstellen geschlossen werden. Dadurch sollte auch der Zugriff des Täters zu dem Ziel-System unterbunden werden.[22]



Botnet: Durch Schadprogramme werden Bots auf Computer eingeschleust und zu einem Netzwerk zusammengeschlossen. Die Computer agieren ferngesteuert und werden zu Zwecken des Angreifers missbraucht.

Phase 7 | «Actions on Objectives» – Aktionen im Zielsystem

Angriffsstrategie

In der letzten Phase hat der Angreifer Zugriff auf das Zielsystem und vollzieht spezifische Aktionen. Sie reichen von der Spionage hin zur Sabotage und dem Datendiebstahl. Zudem möchte der Angreifer immer tiefer in das System eindringen und sein Zielvorhaben zum Abschluss bringen.

Verteidigungsstrategie

In der letzten Phase ist bereits der Worst-Case eingetroffen und es muss zeitnah entschieden werden, welche Handlungen durchzuführen sind. An dieser Stelle ist es hilfreich, wenn bereits ein Notfallprogramm definiert ist. Darunter fallen die Zuständigkeiten personeller Art, aber auch die zu folgenden technischen Abläufe wie Analysen der IT-Forensik.[23]

Wie sinnvoll ist die Cyber Kill Chain?

Die Cyber Kill Chain kann eine der vielen Möglichkeit darstellen, wie ein Angreifer vorgeht. Dennoch muss beachtet werden, dass Cybersicherheit nicht immer so einfach modellierbar ist, wie es hier dargestellt wird und das Modell nicht 1:1 die Realität abbilden kann. Insbesondere in den ersten beiden Phasen der Cyber Kill Chain kann es schwierig sein, den potentiellen Angriff zu bemerken und geeignete Gegenmaßnahmen festzulegen.

Die Komplexität der Angriffe nimmt stetig zu. Bei Advanced Persistent Threats handelt es sich um Angriffsarten, die vielschichtig und innovativ sind und bei denen die Verteidigung durchaus schwieriger sein kann. Die Cyber Kill Chain kann hier zwar ebenfalls genutzt werden, um die Strukturen des Angriffs phasenweise zu analysieren, allerdings ist das Modell zu statisch, um effektiv für APT eine Anwendung zu finden.

Kritisch kann auch betrachtet werden, dass sich nicht alle Angriffsformen mit der klassischen Cyber Kill Chain abbilden lassen, wie das beispielsweise bei Insiderangriffen oder Ransomware der Fall ist. Bei Insiderangriffen verfügt der Täter bereits über wichtige Informationen oder Berechtigungen und bei Ransomware tritt der Täter im Gegensatz zu Malware-Attacken direkt mit dem Opfer in Kontakt. Der Zugang und die Kontrolle über das Zielsystem ist bereits sichergestellt und wird erst nach der Zahlung eines Lösegeldes wieder freigegeben. Außerdem laufen die Attacken automatisiert ab und durchlaufen nicht die einzelnen Phasen der Cyber Kill Chain. Es ist daher nötig, diese Angriffsform für ein besseres Verständnis getrennt zu analysieren und geeignete Maßnahmen zu definieren.

Generell sollten Unternehmen immer alle möglichen Angriffsarten betrachten, damit sie ihre wertvollen Informationen umfassend schützen können.

Prävention ist der beste Schutz

Cyberangriffe und Wirtschaftsspionage sind Bedrohungen, die Unternehmen über alle Größen und Branchen hinweg betreffen. In Zeiten der zunehmenden Digitalisierung treten auch vermehrt Risiken auf, die Unternehmen so nicht einkalkulieren. Die Nutzung mobiler Geräte, eine Bandbreite an Apps und zentrale Logins für Unternehmenskonten machen es Kriminellen einfach, in Zielsysteme einzudringen. Außerdem werden häufig sensible Daten in Cloud-Diensten gespeichert oder Mitarbeiter geben Unbefugten unwissentlich Zugriff auf Daten (Social Engineering).

Cyberbedrohungen werden zunehmend komplexer, wodurch es schwer sein kann, kriminelle Angriffe rechtzeitig zu erkennen und gezielt zu reagieren. Dies führt auch zu einer immer komplexer werdenden Verwaltung von Unternehmenssicherheit. Folglich ist es wichtig, Systeme und Netzwerke präventiv zu schützen und eine Sicherheitsstrategie aufzubauen. Sicherheit verfolgt immer das Ziel zur Risikominimierung und der Sicherung unternehmerischer Prozesse und der gesamten Wertschöpfung. Sicherheit heißt somit auch, das Ziel der langfristigen Sicherung des materiellen Vermögens, geistigen Eigentums und des Kundenvertrauens. Es ist elementar, ein Verständnis für IT-Sicherheit und eine Sicherheitskultur zu schaffen. Diese muss etabliert werden und mit dem Unternehmen organisch wachsen, um langfristig erfolgreich zu sein.

Ein umfassendes Risikomanagement ist ein grundlegender Bestandteil einer fundierten Sicherheitsstrategie von Unternehmen. Es sollte ein Bewusstsein für die vorhandenen Informationen und Daten geschaffen und ein mögliches Verlustrisiko kalkuliert werden. Definieren Sie eine Vertraulichkeitsstufe von Daten und ordnen Sie diese dahingehend in Kategorien ein, wie hoch ein Verlustrisiko ist.[24]

Untersuchen Sie Soft- und Hardware, Daten und Identitätsverwaltung auf mögliche Sicherheitslücken hin. Nur so sind Sie dem Angreifer einen Schritt voraus und können diese Schwachstellen im Voraus eliminieren. Solche Überprüfungen sind als wiederkehrende Schritte innerhalb der Sicherheitsstrategie zu verstehen und stets auf neue Risiken hin zu testen. Achten Sie immer auf die notwendige Transparenz und Kontrolle, um Risiken frühzeitig zu erkennen und nachhaltige Sicherheitsrichtlinien festzulegen.

Social Engineering: Hierunter werden Manipulationen von Personen verstanden, die das Ziel verfolgen, von diesen vertrauliche Informationen zu erhalten, um letztlich in fremde Systeme einzudringen.

Im Rahmen ihrer Sicherheitsstrategie sollten sich Unternehmen heute gezielte Fragen stellen. Diese umfassen die Hauptziele des präventiven Schutzes, das Identifizieren von Angriffen und das Reagieren auf Bedrohungen. Nachfolgend finden Sie eine Auswahl der wichtigsten Fragen:

Präventiver Schutz

Wer greift mit welchen Geräten auf das Unternehmensnetzwerk zu?

Welche Apps werden verwendet und welche Daten nutzen Sie?

Kann der Datenzugriff nicht autorisierter Benutzter eingeschränkt werden?

Wer erstellt Daten und mit wem werden sie geteilt?

Gibt es eine Klassifizierung für Daten?

Ist eingesetzte Software aktuell und sind Sicherheitsupdates installiert?

Identifizieren von Angriffen

Verfügt das Unternehmen über Tools, um einen Angriff zu identifizieren?

Können der Angriff und seine Folgen analysiert werden?

Gibt es Lösungen, um ein weiteres Vordringen des Angreifers abzuwehren?

Reaktion auf Angriffe

Existieren Notfallpläne für den Ernstfall?

Wie kann der Schaden begrenzt werden?

Wie erfolgt die Kommunikation mit Mitarbeitern, Kunden oder Lieferanten?

IT-Sicherheit ist mehr als nur ein Passwort

Unternehmen sollten ihre bereits eingesetzten Software-Lösungen daraufhin untersuchen, ob sie Attacken entlang der Phasen der Cyber Kill Chain standhalten könnten. Diskutieren Sie alternativ diese Punkte proaktiv mit dem Anbieter Ihrer Software-Lösungen.

Bei der Auswahl neuer Lösungen sollten Sie sich fragen, ob Sie etwas auslagern wollen und können.

Möglichkeit zur Auslagerung

IT Forensik
Ist der Ernstfall eingetreten, werden Angriffe dokumentiert und analysiert und mittels digitaler Spuren der Täter ermittelt.

Security Operations Center
Zentrum aus IT-Spezialisten, welches Cybe drohungen rechtzeitig erkennt und abwehr IT-Infrastruktur und Daten vor in- und exte Gefahren schützt.

Intrusion Detection System
Kann die Firewall ergänzen und überwa Netzverkehr, um so Angriffe systema erkennen.

Security Information and Event Management (SIEM)
Es werden Analysen in Echtzeit bereitgestellt und sicherheitsgefährdende Ereignisse behandelt.

Möchten Sie Ressourcen in der Cloud, On-Premise oder mittels einer Hybridumgebung bereitstellen? Egal, für welches Szenario Sie sich entscheiden, beachten Sie, dass Sie Lösungen für alle relevanten Bereiche in Ihrem Unternehmen finden. Darunter fällt die Identitätskontrolle, die Sicherung von Geräten, Ihrer IT-Infrastruktur und der Schutz von Programmen und Daten. Beachten Sie daher bei der Auswahl geeigneter Soft- und Hardware-Lösungen folgende Funktionen:

Identitätssicherung

- Prüfung von Nutzeridentitäten vor dem Netzwerkzugriff
- Möglichkeit zur Einschränkung von Datenzugriff anhand definierter Richtlinien
- Einsatz von Multi-Faktor-Authentifizierung

Schadsoftware

- Blockieren unerwünschter Downloads
- Erkennung von Phishing-Websites und Schadsoftware

Cyberangriffe

- Bereitstellung wichtiger Informationen über den Ort des Angriffs und Aktionen des Angreifers sowie Reaktionsempfehlungen
- Software zur Analyse komplexer Angriffe und interne Bedrohungen wie z.B. Advanced Threat Protection

Programme & Daten (ICON)

- Schutz von E-Mails, Informationen und Daten On-Premise und in der Cloud
- Schutz vor ungewollter Datenfreigabe an Unbefugte wie z.B. Data Loss Prevention
- Compliance-Kontrolle durch automatische Datenklassifizierung und -filterung

Unternehmen in der Verantwortung

Mittelständische Unternehmen werden zunehmend Opfer von Cyberangriffen. Trotz dieses steigenden Risikos und des zunehmenden Bewusstseins für die Dringlichkeit, mehr in Informationssicherheit zu investieren, werden Gegenmaßnahmen bisher unzureichend umgesetzt.

Unternehmen sind in höherem Maße gefordert, auf die neuen Sicherheitsanforderungen zu reagieren, um nicht den Verlust von Betriebsgeheimnissen und das Vertrauen von Geschäftspartnern und Kunden zu verlieren.

Die Cyber Kill Chain gibt ein Verständnis, wie Angreifer in der Regel vorgehen. Sie liefert ferner die Möglichkeit, bereits eingesetzte Software auf ihre Abwehrmöglichkeiten hin zu untersuchen. Wir empfehlen an erster Stelle jedoch einen ganzheitlichen Ansatz. Etablieren Sie eine Sicherheitsstrategie in Ihrem Unternehmen. Definieren Sie Zuständigkeiten, überprüfen Sie technische Ressourcen und definieren Sie einen Notfallplan für die Reaktion auf kritische Vorfälle. Das ermöglicht im Ernstfall schnell reagieren zu können. Cyberkriminalität ist immer in Bewegung. Was heute gilt, kann morgen bereits überholt sein. Es ist daher wichtig, stets die aktuellen Sicherheitsmaßnahmen zu überprüfen und an aktuelle Bedrohungen anzupassen.

Ansprechpartner

Uwe Gierstorfer

Sales Executive Cloud Solutions I +49 681 98915 284 I uwe.gierstorfer@dataone.de

Literaturverzeichnis

Bundesamt für Sicherheit und Informationstechnik (2017), Cyber-Sicherheits-Umfrage 2017. Cyber-Risiken, Meinungen und Maßnahmen. Online unter https://www.bsi.bund.de/SharedDocs/Downloads/ACS/cyber-sicherheits-umfrage_2017.pdf?__blob=publicationFile&v=3

Kaspersky (2017), The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within. Online unter: https://www.kaspersky.com/blog/the-human-factor-in-it-security/

Nicolai Kwasniewski (2017), Cyberangriffe auf Unternehmen. Ein Hack, eine versetzte Schweißnaht – fatale Folgen. In: Spiegel Online. 30.11.2017. Online unter http://www.spiegel.de/wirtschaft/unternehmen/cyberangriffe-so-gefaehrdet-ist-die-deutsche-wirtschaft-a-1178050.html

Lockheed Martin (2015), Gaining the Advantage. Applying Cyber Kill Chain Methodology to Network Defense. Online unter: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf

PricewaterhouseCoopers (2017), Im Visier der Cyber-Gangster. So gefährdet ist die Informationssicherheit im deutschen Mittelstand. Online unter: https://www.pwc.de/de/mittelstand/assets/it-sicherheit-im-mittelstand-neu.pdf

Radware (2018), 2018 Executive Application and Network Security Report. Online unter: https://www.radware.com/c-suite-2018/

SonicWall (2018), 2018 SonicWall Cyber Threat Report, Mid-Year Update. Online unter: https://www.sonicwall.com/de-de/lp/2018-cyber-threat-report

SonicWall (2018), SonicWall Cyber Threat Report: aktuelle Bedrohungsanalyse für das erste Halbjahr 2018. Pressemitteilung vom 11.07.2018. Online unter: https://www.presseportal.de/pm/59729/3994624

Standford University (2018), Risk Classifications. Online unter: https://uit.stanford.edu/guide/riskclassifications

Endnoten

[1] SonicWall (2018), 2018 SonicWall Cyber Threat Report, Mid-Year Update. Online unter: https://www.sonicwall.com/de-de/lp/2018-cyber-threat-report

[2] Ebd. S.4-5.

[3] SonicWall (2018), SonicWall Cyber Threat Report: aktuelle Bedrohungsanalyse für das erste Halbjahr 2018. Pressemitteilung vom 11.07.2018. Online unter: https://www.presseportal.de/pm/59729/3994624

[4] Bundesamt für Sicherheit und Informationstechnik (2017), Cyber-Sicherheits-Umfrage 2017. Cyber-Risiken, Meinungen und Maßnahmen. S.7. Online unter https://www.bsi.bund.de/SharedDocs/Downloads/ACS/cyber-sicherheits-umfrage_2017.pdf?__blob=publicationFile&v=3

[5] Konkret betrug die Schadsumme 65 Milliarden Dollar. Weltweit waren im Jahr 2017 230.000 Unternehmen betroffen mit einer gesamten Schadsumme von 450 Milliarden Dollar. Nicolai Kwasniewski (2017), Cyberangriffe auf Unternehmen. Ein Hack, eine versetzte Schweißnaht – fatale Folgen. In: Spiegel Online. 30.11.2017. Online unter: http://www.spiegel.de/wirtschaft/unternehmen/cyberangriffe-so-gefaehrdet-ist-die-deutsche-wirtschaft-a-1178050.html

[6] Bundesamt für Sicherheit und Informationstechnik (2017), Cyber-Sicherheits-Umfrage 2017. Cyber-Risiken, Meinungen und Maßnahmen. S.6, S.8. Online unter https://www.bsi.bund.de/SharedDocs/Downloads/ACS/cyber-sicherheits-umfrage_2017.pdf?__blob=publicationFile&v=3

[7] Bundesamt für Sicherheit und Informationstechnik (2017), Cyber-Sicherheits-Umfrage 2017. Cyber-Risiken, Meinungen und Maßnahmen. S.6. Online unter https://www.bsi.bund.de/SharedDocs/Downloads/ACS/cyber-sicherheits-umfrage_2017.pdf?__blob=publicationFile&v=3

[8] Radware (2018), 2018 Executive Application and Network Security Report. Online unter: https://www.radware.com/c-suite-2018/

[9] Bundesamt für Sicherheit und Informationstechnik (2017), Cyber-Sicherheits-Umfrage 2017. S.13-14.

[10] PricewaterhouseCoopers (2017), Im Visier der Cyber-Gangster. So gefährdet ist die Informationssicherheit im deutschen Mittelstand. Hier: S.4. Online unter: https://www.pwc.de/de/mittelstand/assets/it-sicherheit-im-mittelstand-neu.pdf

[11] Die Zahl bezieht sich auf die Budgets zwischen 100.000 und 1 Million Euro. Ebd. S.7.

[12] Kaspersky (2017), The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within. Online unter: https://www.kaspersky.com/blog/the-human-factor-in-it-security/

[13] Lockheed Martin (2015), Gaining the Advantage. Applying Cyber Kill Chain Methodology to Network Defense. S.7.

[14] Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste (2017), Aktuelle Lage der IT-Sicherheit in KMU. Hier: S.45. Online unter: https://www.wik.org/fileadmin/Sonstige_Dateien/IT-Sicherheit_in_KMU/WIK-Studie_Aktuelle_Lage_der_IT-Sicherheit_in_KMU_Langfassung__2_.pdf

[15] Lockheed Martin (2015), Gaining the Advantage. Applying Cyber Kill Chain Methodology to Network Defense. Online unter: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf

[16] SonicWall (2018), SonicWall Cyber Threat Report: aktuelle Bedrohungsanalyse für das erste Halbjahr 2018.

[17] Lockheed Martin (2015), Gaining the Advantage. Applying Cyber Kill Chain Methodology to Network Defense. S.12.

Endnoten

[18] Lockheed Martin (2015), Gaining the Advantage. Applying Cyber Kill Chain Methodology to Network Defense. S.4.

[19] Ebd. S.5.

[20] Ebd. S.6.

[21] Lockheed Martin (2015), Gaining the Advantage. Applying Cyber Kill Chain Methodology to Network Defense. S.8.

[22] Ebd. S.9.

[23] Ebd. S.10.

[24] Es hat sich eine Einteilung ist Daten mit geringen, moderatem und hohem Risiko etabliert. Vgl. dazu: Standford University (2018), Risk Classifications. Online unter: https://uit.stanford.edu/guide/riskclassifications

[25] Vgl. dazu: Amrit T. William / Mark Nicolett ([2005]), Improve IT Security with Vulnerability Management. Gartner Research. Online unter: https://www.gartner.com/doc/[480703]/improve-it-security-vulnerability-management