DataGuard

E-BOOK

IN 10 SCHRITTEN ZU CYBER-SICHERHEIT

IN 10 SCHRITTEN ZU CYBERSICHERHEIT

EINFÜHRUNG

2012 hat die britische Regierung ein Dokument mit dem Titel „10 Steps to Cybersecurity" (10 Schritte zur Erlangung von Cybersicherheit) veröffentlicht – eine Schritt-für-Schritt-Anleitung mit praktischen Empfehlungen, die jedes Unternehmen umsetzen kann, um die Sicherheit seiner Netzwerke und Daten zu erhöhen.

Um der erhöhten Risikolage durch Cybergefahren Rechnung zu tragen und den Organisationen die wirksamsten Sicherungsmaßnahmen an die Hand zu geben, wurden diese „10 Schritte zur Erlangung von Cybersicherheit" für 2022 aktualisiert. In diesem Artikel gehen wir auf jeden dieser Schritte im Einzelnen ein und zeigen, welche Bedeutung er für die allgemeinen Unternehmensvorgänge hat.

WORUM GEHT ES BEI CYBERSICHERHEIT?

Als „Cybersicherheit" bezeichnet man den Schutz von Systemen, die mit dem Internet verbunden sind, vor den damit verbundenen Gefahren. Sie spielt außerdem eine wesentliche Rolle bei der Abwendung von Angriffen, die darauf abzielen, den Betrieb eines Systems oder Gerätes zu stören oder zu blockieren. Mit der steigenden Anzahl von Anwendern, Geräten und Programmen innerhalb moderner Organisationen steigt auch der Bedarf an Cybersicherheit. Da mittlerweile mehr und mehr sensible Daten im Online-Raum kursieren, nehmen auch Cyberattacken und angewandte Angriffstechniken zu.

Eine Cybersicherheitsstrategie, die auf festen Säulen steht, kann Organisationen jedoch wirksam gegen böswillige Angriffe absichern. In diesem Blog erfahren Sie mehr über das Zusammenspiel zwischen Cybersecurity und Informationssicherheit. Die „10 Schritte zur Erlangung von Cybersicherheit" stellen einen Maßnahmenkatalog vor, der Schutz vor Attacken und vor wirtschaftlichen oder Imageschäden bieten kann. Die „10 Schritte zur Erlangung von Cybersicherheit" stellen einen Maßnahmenkatalog vor, der Schutz vor Attacken und vor wirtschaftlichen oder Imageschäden bieten kann.

WORIN BESTEHEN DIE 10 SCHRITTE ZUR CYBERSICHERHEIT?

In jedem Unternehmen, das sich in irgendeiner Weise auf Digitaltechnologien stützt, ist Cybersicherheit essenziell. Wenn Sie sich fragen, wie Sie die nötige Absicherung am besten erlangen können, geben die nachfolgenden 10 Schritte wertvolle Anhaltspunkte.

1. RISIKOMANAGEMENT

Im Kontext der Cybersicherheit hilft Risikomanagement bei der Absicherung der Technologien, Systeme und Daten einer Organisation, indem es dafür sorgt, dass diese Absicherung, in der am besten geeigneten Weise erfolgt. Außerdem trägt Risikomanagement dazu bei, dass die Ressourcen auf die wesentlichen Bereiche des Unternehmens fokussiert werden. Eine wirksame Strategie für das Risikomanagement ist engmaschig in das Netzwerk der Organisation eingewoben und geht Hand in Hand mit den Maßnahmen, die zur Kontrolle anderer Gefahren eingesetzt werden.

Damit die Strategie wirkt, gilt es im Vorfeld zu überlegen, in welchem größeren Kontext die Cyberrisiken gemanagt werden sollen und wo es sinnvoll ist, Cyberrisikomanagement zu betreiben und wo nicht. Anschließend muss hierfür ein Risikomanagement-Ansatz ausgewählt werden, der zum Unternehmen passt, und dieser effektiv an alle von ihm Betroffenen kommuniziert werden.

2. EINBINDUNG UND SCHULUNG

Im Zentrum jeder Cybersicherheitsrichtlinie sollte stets der Mensch stehen. Gute Sicherheitspraktiken berücksichtigen immer auch die Arbeitsweise der Belegschaft und behindern diese nicht. Ihre Belegschaft ist Ihr effektivster Abwehrschild (oder im Ernstfall Ihr wichtigster Detektor) bei Bedrohungen, vorausgesetzt, sie wird adäquat eingebunden. Sie sollten eine starke Cybersicherheitskultur entwickeln, die zum Melden von Verdachtsfällen und Problemen ermutigt. Mittels Bewusstseinsschärfung oder Schulungen kann sich die Belegschaft die nötigen Kenntnisse aneignen, um ihre Aufgaben effizient und dennoch sicher auszuführen. Abgesehen davon, dass dies das Unternehmen schützt, vermittelt ein solches Vorgehen Wertschätzung gegenüber den Mitarbeitenden und ihrem Beitrag, den sie im Unternehmen leisten.

Wichtig ist, das höhere Management zu ermutigen, mit gutem Beispiel voran zu gehen und eine effektive Kommunikation zu allen Teammitgliedern aufzubauen. Eine gute Strategie ist, interne Kampagnen durchzuführen, die das Bewusstsein für Sicherheitsbedrohungen schärfen, und die Cybersicherheitstrainings auf die spezifischen Gegebenheiten im Unternehmen anzupassen.

3. ASSET-MANAGEMENT

Das Asset-Management, also die Verwaltung der „Vermögenswerte“ im weitesten Sinne, ist der Vorgang, mit dem alle nötigen Informationen zu vorhandenen Assets erfasst und aufbewahrt werden. Natürlicherweise neigen Systeme über längere Zeiträume dazu sich auszudehnen. Dies erschwert, alle Ressourcen einer Umgebung immer auf dem neuesten Stand zu halten.

Services, bei denen die Patches fehlen, Konten für Cloudspeicher, deren Zugangsdaten nicht mehr sicher sind, oder falsch klassifizierte Dokumente sind alles Beispiele für Umgebungen, in denen Zwischenfälle auftreten können, weil die Umgebung nicht gründlich im Blick behalten werden kann. Es ist aber essenziell, diese Assets alle im Blick zu haben, um die mit ihnen verbundenen Risiken abschätzen und mindern zu können. Sie müssen beispielsweise wissen, wann ein Anbieter die vorhandenen Softwaresysteme nicht mehr unterstützt, damit Sie nicht plötzlich mit Legacy-Systemen arbeiten, die mehr und mehr Einfallstore bieten.

Die Lösung: Sie integrieren Asset-Management in Ihre Systeme. Hierzu ermitteln Sie zunächst, welche Services und Funktionen innerhalb der Umgebung kritisch sind. Damit Sie diese priorisieren können, sehen Sie sich an, welche Daten zu ihnen gehören und zu welchen Technologien Abhängigkeiten bestehen. Ständige Wissenserweiterung sollte ebenso Bestandteil sein wie das Aufräumen – behalten Sie nur die Daten, die Sie benötigen.

4. ARCHITEKTUR UND KONFIGURATION

Wir leben in einer Welt, die sich ständig ändert, insbesondere im Hinblick auf Technologien und Cybersicherheit. Unternehmenssysteme müssen daher von Anfang an mit solider Cybersicherheit ausgestattet werden und auch mit neuen Gefahren und Bedrohungen mithalten können. Dies bedeutet, dass sie ständig aktualisiert und auf dem neuesten Stand gehalten werden müssen.

Machen Sie sich zunächst klar, welche Art von System Sie aufbauen wollen und zu welchem Zweck. Gestalten Sie das System so, dass es sich leicht aktuell halten lässt, aber nur schwer kompromittierbar oder angreifbar ist. Sollte es zu einem Zwischenfall kommen, muss es leicht gehen, Ursachen oder Einfallstore aufzudecken und sie genauer zu untersuchen.

5. IT-SCHWACHSTELLENMANAGEMENT

Hacker nutzen öffentlich bekannte IT-Schwachstellen oder Systemfehler aus, um sich Zugang zu Systemen und Netzwerken zu verschaffen. Sobald eine Schwachstelle publik wird, werden Angreifer versuchen sie auszunutzen, meistens wahllos. Daher ist es für die Sicherheit von Unternehmenssystemen absolut kritisch, Sicherheitsupdates unmittelbar nach ihrer Veröffentlichung zu installieren. Gleiches gilt für alle Systeme, die über das Internet angegriffen werden könnten. Manche Schwachstellen sind schwerer zu beheben als andere. Die Kritischsten haben Priorität. Zu wissen, welche dies sind, gehört zu einer starken IT-Schwachstellenmanagement-Strategie.

Diese drei Dinge sollten Sie auf jeden Fall tun:

1. Halten Sie Ihre Systeme aktuell.
2. Entwickeln Sie einen Prozess für das IT-Schwachstellenmanagement.
3. Behalten Sie ein Auge auf Ihre Legacy-Systeme.

6. IDENTITÄTS- UND ZUGRIFFSMANAGEMENT

Der Zugriff auf Systeme und Dienste muss geschützt sein. Genauso wichtig ist zu definieren, wer oder was unter welchen Umständen Zugriff benötigt und erhält. Damit eine effektive Zugangskontrolle möglich ist, müssen Anwender, Geräte oder Systeme zuverlässig identifiziert und ihre Berechtigung nachgewiesen werden können. Mit einer wirksamen Strategie für das Identitäts- und Zugriffsmanagement haben Angreifer es schwer; berechtigte Nutzer können hingegen sehr unproblematisch auf benötigte Ressourcen zugreifen.

Es gibt einige Dinge zu beachten, wenn es um die Einrichtung von Richtlinien und Prozessen für das Identitäts- und Zugriffsmanagement geht. Multi-Faktor-Authentifizierung (MFA) für alle Benutzerkonten sollte ebenso dazugehören wie MFA plus zusätzliche Zugangskontrollen für privilegierte Konten. Außerdem sollte die Umgebung ständig auf potenzielles böswilliges Verhalten hin überwacht werden, um nur einige wenige zu nennen.

7. DATENSICHERHEIT

Daten zu schützen bedeutet, dass niemand sie ohne die entsprechenden Schreibrechte verändern oder löschen kann. Dies schließt ein, dass die Daten auch während ihrer Übertragung oder im Ruhezustand sicher geschützt sind und am Ende ihres produktiven Lebens sicher aus dem Verkehr gezogen werden (durch sicheres Löschen bzw. Zerstörung des Mediums, auf dem sie gespeichert waren). Da Sie möglicherweise keine absolute Kontrolle über die Daten haben, sollten Sie sich Schutzmechanismen überlegen, die Sie einführen könnten, genauso auch Garantien, die Sie möglicherweise in unterschiedlichen Szenarien von Dritten benötigen.

Eine weitere wichtige Sicherheitsvorkehrung sind Backups. Sie sollten stets aktuell sein, getrennt und offline aufbewahrt werden (3-2-1-Regel) und alle wichtigen Daten enthalten. Denn Ransomware-Angriffe nehmen zu und werden immer gezielter.

8. PROTOKOLLIERUNG UND ÜBERWACHUNG

Wenn Sie ein klares Bild gewinnen möchten, wie Ihre Systeme genutzt werden, müssen Sie alle Aktivitäten fortlaufend protokollieren. Sagen wir mal, Sie haben einen Sicherheitsvorfall oder Verdacht. Gute Protokollierungspraktiken erlauben Ihnen in

einem solchen Fall, Einsicht in den Hergang zu nehmen und zu analysieren, welche Auswirkungen er auf Ihr Unternehmen hatte oder noch hat. Durch aktives Überwachen („Monitoring“) der Protokolle lassen sich Warnzeichen, wie bekannte Angriffsmuster oder ungewöhnliches Systemverhalten, erkennen. Bei Auffälligkeiten, die auf einen Sicherheitsvorfall hindeuten, können Sie zügig Abwehrmaßnahmen einleiten, um die Auswirkungen möglichst gering zu halten. Das ist hier mit Überwachung der Sicherheit gemeint.

Sie können aus Ihren Protokollen Erkenntnisse ziehen und daraus Pläne zur Vorfallserkennung und -behandlung ableiten, um sich gezielt auf Vorfälle vorzubereiten, was in der Zukunft sehr nützlich sein könnte. Nutzen Sie intelligente Funktionen zur Erkennung von Sicherheitsgefahren, um Ihre Cybersicherheit möglichst wasserdicht zu machen.

9. VORFALLSMANAGEMENT

Infolge eines IT-Vorfalls („Incident“) können Unternehmen viel verlieren: Zeit, Geld oder Ansehen. Gutes Vorfallsmanagement kann die Schäden eines Vorfalls gering halten. Wird sein Auftreten sofort erkannt und schnellstmöglich mit geeigneten Maßnahmen gebannt, lassen sich die finanziellen und betrieblichen Auswirkungen reduzieren. Ein Imageschaden fällt geringer aus, wenn die Situation aus Sicht der Presse richtig gehandhabt wurde. Wenn Sie dann auch noch das aus einem Vorfall Gelernte in die Praxis umsetzen, sind Sie zukünftig auf ähnliche Situationen wesentlich besser vorbereitet.

Um wirklich auf jeden Fall der Fälle vorbereitet zu sein, müssen Sie Ihre definierten Abwehrmaßnahmen mit Ihrer Belegschaft eintrainieren und proben und das daraus Gelernte zur organisatorischen Verbesserung mit einfließen lassen.

10. SICHERHEIT INNERHALB DER LIEFERKETTE

Ein Großteil der Unternehmen bezieht Produkte, Systeme und Services von Anbietern oder Zulieferern, die direkt in die Lieferkette eingebunden sind. Ist einer dieser Lieferanten Ziel eines Cyberangriffs, kann sich dies in gleicher Weise auf das Unternehmen auswirken, so als wäre es selbst das Angriffsziel. Umfangreiche oder komplexe Lieferketten abzusichern ist nicht immer so leicht, da in jedem Glied innerhalb dieser Kette eine IT-Schwachstelle auftreten oder ausgenutzt werden könnte.

Daher besteht der erste Schritt darin, die Lieferkette nachzuvollziehen. Zu ihr gehören allgemeine Dienstleister wie Cloud-Serviceprovider genauso wie Lieferanten, mit denen Sie Einzelverträge geschlossen haben. Sicherer machen Sie Ihre Lieferkette, wenn Sie Kontrolle über sie haben und sie fortlaufend verbessern.

FAZIT

Das übergeordnete Ziel der hier vorgestellten 10 Schritte besteht darin, Unternehmen bei der Handhabung von Cybersicherheitsrisiken zu unterstützen. Dazu wurden die Schutzmechanismen in 10 Komponenten aufgebrochen. Werden die genannten Sicherungsmaßnahmen ergriffen, ist es wesentlich unwahrscheinlicher, dass ein Cyberangriff auftritt. Außerdem minimieren sie die Auswirkungen auf das Unternehmen, sollte es doch einmal dazu kommen.

Diese Art von Risikominderung versetzt Sie in eine bessere Ausgangslage, um im Ernstfall adäquat reagieren zu können, den Betrieb schneller wieder aufzunehmen und zufriedene Bestandskunden zu halten, was übrigens wesentlich kostengünstiger ist als Neukunden zu gewinnen. Dies bedeutet nicht, dass Ihr Wachstum auf der Stelle tritt. Cybersicherheit ist Neukunden wichtig und daher für sie äußerst attraktiv – sie wird Ihrem Geschäftswachstum daher eher zuträglich sein.

DataGuard ist ein Compliance-Software-Unternehmen mit Fokus auf Datenschutz und Informationssicherheit. Als einer der europäischen Marktführer im Bereich Compliance-SaaS ermöglicht DataGuard Tausenden KMU und Großunternehmen die unkomplizierte Operationalisierung von Datenschutz (Privacy), Informationssicherheit und Compliance (kurz: „PIC"). Mit seiner Komplettlösung reduziert DataGuard für Unternehmen Zeit und Kosten bei der Einhaltung von Datenschutzgesetzen wie der DSGVO, der Einholung und Verwaltung von Einwilligungen und Präferenzen oder beim Erhalten von Zertifizierungen wie der ISO 27001. So können sich Kunden auf ihr Kerngeschäft konzentrieren, Mehrwert durch Vertrauen und Compliance schaffen und gleichzeitig Risiken minimieren. DataGuard hat Standorte in München, Berlin, London und Wien.

Jetzt Termin vereinbaren, um über Ihre Herausforderungen zu sprechen und erste Schritte zu definieren:

Erstgespräch buchen

Weiterführende Ressourcen:

→ **Cyber- und Informationssicherheit - Hier liegen die Unterschiede**

→ **Informationssicherheit im Überblick: Definition, Schutzziele, Aufgaben**

→ **Informationssicherheits-Managementsystem im Überblick**

dataguard.de kontakt@dataguard.de +49 89 452 459-900

DataGuard