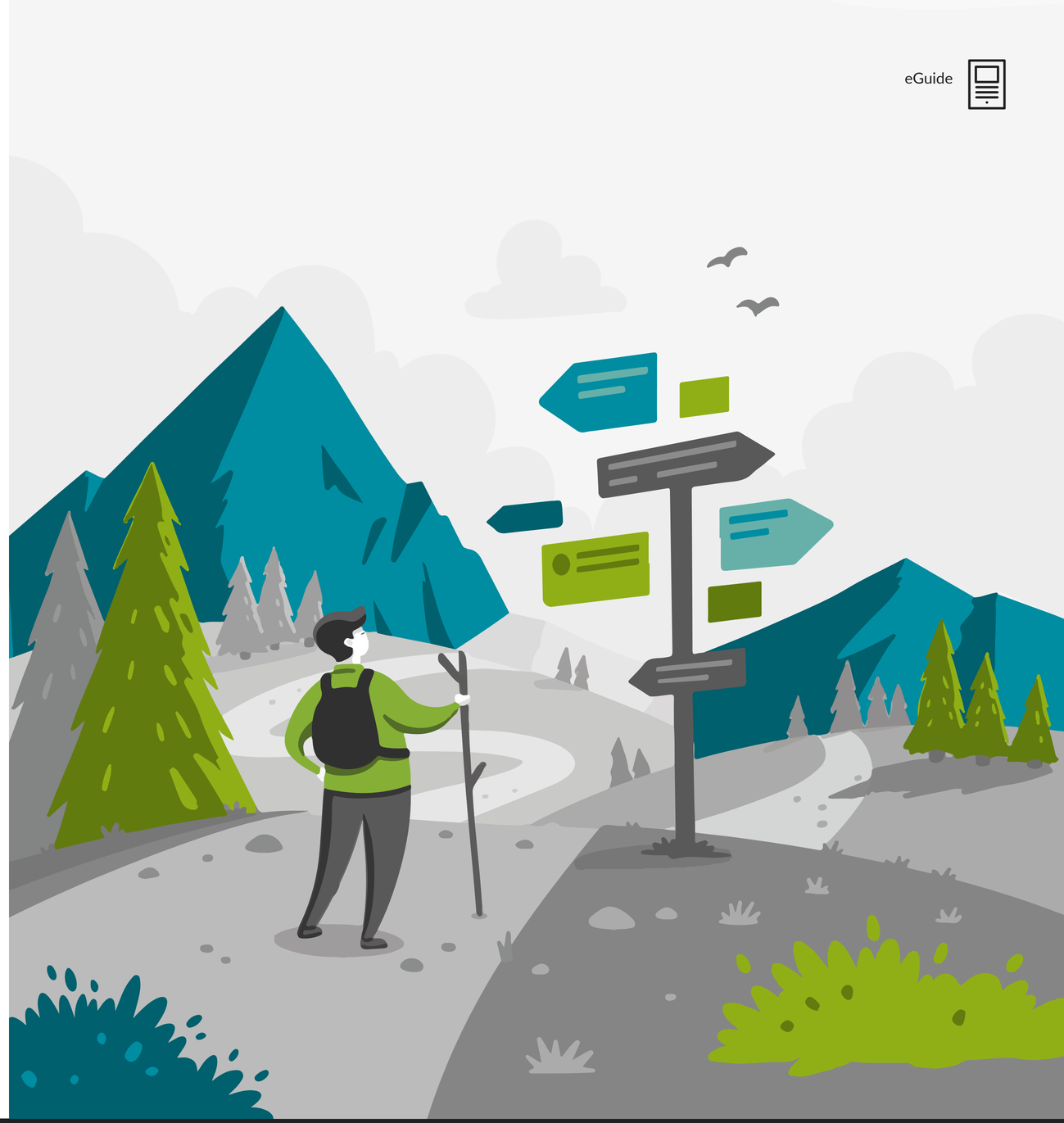
Einführung in die Grundlagen der Cybersicherheit.

Von Trevor Pott
Technical Security Lead, Juniper Networks



Einführung

Themen dieses Dokuments sind die Grundlagen der Informationssicherheit, welche Aufgabe sie haben und warum sie so wichtig sind.

Informationssicherheit oder „InfoSec“ (von „Information Security“) beschreibt alle Aspekte in Bezug auf den Schutz von Informationen: Prinzipien, Werkzeuge, Technologien, technische Umsetzung, Produkte, Dienste und praktische Anwendungen. Informationssicherheit dreht sich um Menschen. Es sind fast ausschließlich menschliche Fehler, die zu Gefährdungen führen.

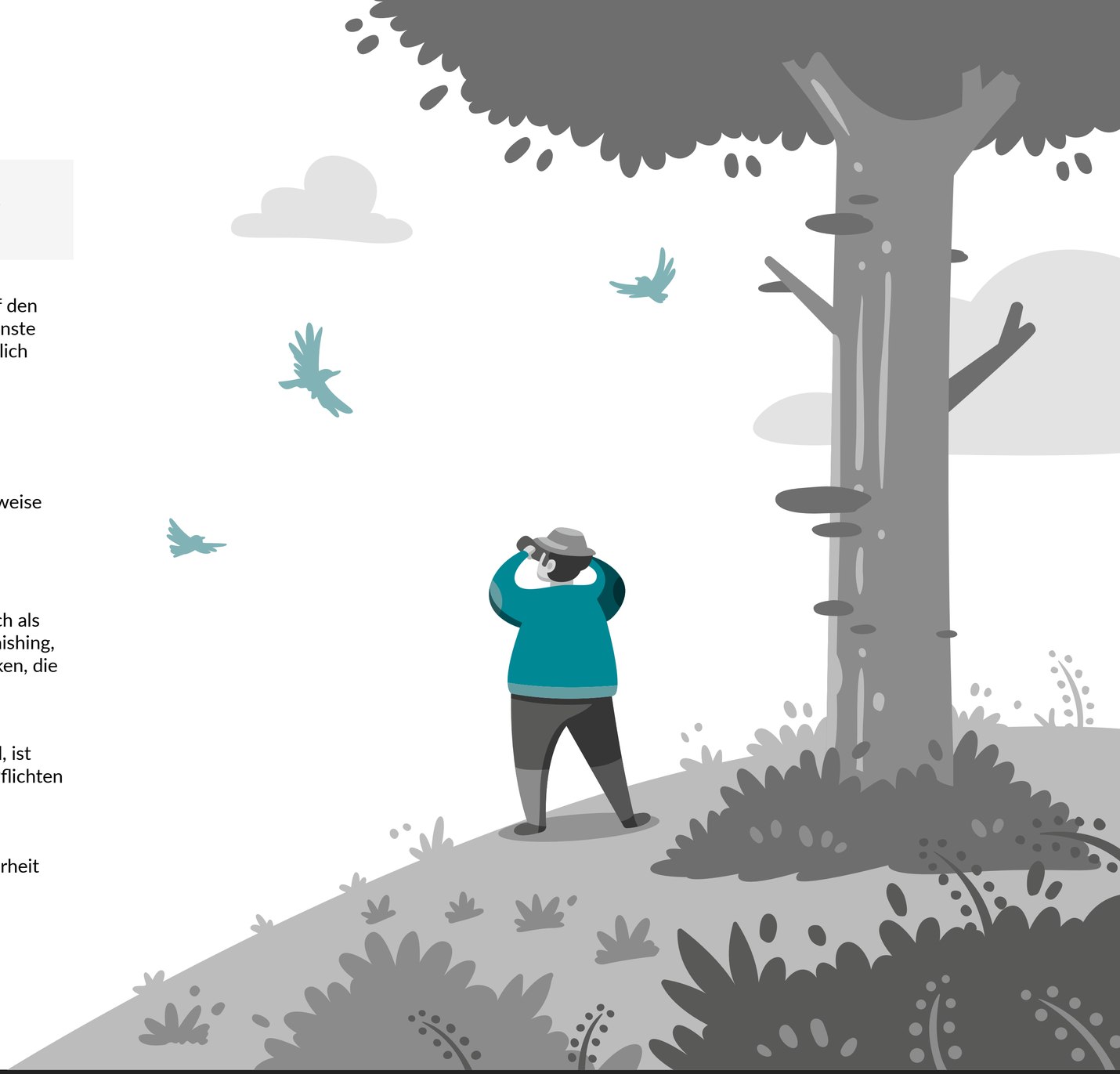
Es gibt drei Hauptursachen der Gefährdung durch Menschen: **Unwissenheit, Social Engineering und Fahrlässigkeit.**

Unwissenheit oder Unkenntnis kann zum Sicherheitsrisiko werden, wenn wir irrtümlicherweise glauben, etwas zu wissen, das wir in Wahrheit nicht kennen.

Social Engineering kann etwas so Einfaches sein wie ein Fake-Anruf durch jemand, der sich als „Microsoft-Techniker“ ausgibt oder etwas so Ausgeklügeltes wie eine E-Mail mit Spear-Phishing, die auf eine nachgebildete Website führt. Es zielt darauf ab, Ihnen Einzelheiten zu entlocken, die Zugriff auf Ihre Benutzerkonten ermöglichen.

Auch wenn wir uns alle des Social Engineering nicht bewusst und daher dafür anfällig sind, ist Fahrlässigkeit eine bewusste Entscheidung. Man muss bereit sein, einige Aspekte seiner Pflichten bei Seite zu legen, wie z. B. sich weiterzubilden oder seinen Aufgaben nachzukommen.

Glücklicherweise kann moderne Technologie genutzt werden, um Gefährdungen der Informationssicherheit durch die Abwehr von Angriffen, die Übermittlung von Erinnerungen an Betreiber und die Erkennung von bösartigem, anormalem oder fahrlässigem Verhalten zu verhindern.



Grundlegende IT-Informationssicherheit

Daten und Metadaten

Die meisten Informationen werden irgendwo als Daten in einem Computer gespeichert, nicht nur in Form von Dateien oder Datenbanken, sondern auch als Bilder, Word-Dokumente, Datensätze usw.

Informationen über Informationen, die als Metadaten bezeichnet werden, sind ebenfalls wichtig.

Mit Bildern sind häufig Metadaten verknüpft, zum Beispiel GPS-Koordinaten oder Details des Geräts, mit dem sie aufgenommen wurden. Werden diese Metadaten nicht vor der Veröffentlichung in den sozialen Medien entfernt, kann jemand, der Böswilliges beabsichtigt, sie verwenden, um den Zielstandort und sogar den Typ des Smartphones zu bestimmen und damit eine Person leichter identifizieren.

Stellen Sie sich jemanden vor, der seine Mahlzeit fotografiert und das Bild auf einem sozialen Medium postet. Ein Dieb könnte dadurch Ort und Zeit schlussfolgern und berechnen, ob diese Person nach Hause zurückkehren könnte, bevor der Dieb seinen Diebstahl vollendet hätte.

Metadaten können auch Firmengeheimnisse offenlegen. Ein Elektroinstallateur, der ein Foto einer gerade abgeschlossenen Verkabelung in einem neuen, noch nicht bekanntgegebenen Datencenter veröffentlicht, könnte leicht seinen Standort unbeabsichtigt an jeden verraten, der sich die Metadaten anschaut. In ähnlicher Weise speichert ein Word-Dokument häufig Verlaufsdaten über alle, die es bearbeitet haben, was rechtliche Folgen haben kann.

Weit mehr als Firewalls und Anti-Malware

Klassische Firewalls und Anti-Malware sind für sich genommen nicht besonders wirksam.

Eine klassische Firewall kann jemanden davon abhalten, Ihren PC fernzusteuern, kann jedoch keine Phishing-E-Mails herausfiltern, in denen ein Link enthalten ist, der beim Anklicken entweder eine Anwendung für die Fernsteuerung herunterlädt, die hinter einer Firewall funktioniert oder Ihre Firewall so umkonfigurieren kann, dass der Fernzugriff auf Ihren PC möglich ist.

Ebenso ist Anti-Malware-Software bei der Verteidigung gegen schädliche Dateien eines bekannten Typs recht gut, nicht jedoch gegen bislang nicht identifizierte. Außerdem ist sie praktisch nutzlos als Schutz vor den unzähligen interessanten Dingen, die über einen Internetbrowser den Weg auf Ihren PC finden.

In Unternehmen konzentrieren sich die meisten InfoSec-Produkte und -Dienste auf Daten, die gerade übertragen werden – mit dem Ziel, alles Bösartige abzufangen, bevor es den Benutzer erreicht oder das Netzwerk verlässt.

Informationssicherheit der nächsten Generation

In den 1990er-Jahren kamen Firewalls in der Anwendungsschicht auf, die als Proxy zwischen einer Anwendung und der Außenwelt fungierten. Darauf folgten Next Generation Firewalls (NGFW), die mehr in die organisatorische Infrastruktur integriert sind und erweiterte Funktionen bieten, wie z. B. die Anwendung von Richtlinien, die nicht nur auf der IP-Adresse, sondern auf Benutzernamen oder -gruppen basieren.

Im Allgemeinen hindert eine NGFW Übeltäter daran, von außen mit einfachen Angriffen in ein Netzwerk vorzudringen. Außerdem bietet sie einige Funktionen für das Scannen von Daten während der Übertragung, wie die Überprüfung von E-Mails auf Phishing-Versuche. NGFWs können Tausende von Benutzern gleichzeitig schützen und Endpunkte verteidigen, bei denen kein Antivirenschutz möglich ist, wie etwa bei Druckern.

Next-Generation Anti-Malware (NGAM) – oder Next-Generation Anti-Virus (NGAV) – kann nur das System schützen, auf dem diese Software installiert ist. Sie wird deshalb in Verbindung mit NGFWs eingesetzt, um gegen Social-Engineering-Angriffe gewappnet zu sein.

Eine NGFW versucht, das Übel gleich an vorderster Stelle von Ihrem PC fernzuhalten, was die beste und sicherste Option ist.

NGAM (oder NGAV) versucht, eine Schädigung Ihres PCs zu verhindern, wenn der Schädling einmal eingedrungen ist, quasi als letzte Verteidigungslinie.

Grundlegende IT-Informationssicherheit

WAF und Anwendungssicherheit

Der nächste Entwicklungsschritt ist die Web Application Firewall (WAF). Eine WAF ist eine Firewall in der Anwendungsschicht, die sich auf per HTTP- und HTTPS-gelieferte Anwendungen konzentriert. Üblicherweise handelt es sich um solche, auf die über das Internet (im Firmennetz oder extern) zugegriffen wird.

WAFs schützen vor spezifischen Schwachstellen einer bestimmten Anwendung oder Klasse von Anwendungen. So kann eine WAF zum Beispiel schädliche SQL-Befehle herausfiltern, um deren Ausführung zu unterbinden. WAFs werden oft betriebsintern verwendet, zum Schutz gegen firmeninterne Bedrohungen und um zu verhindern, dass eine Ebene einer Anwendung durch die Kompromittierung einer anderen beeinträchtigt wird.

Die Anwendungssicherheit stützt sich nicht immer auf Firewalls, Anti-Malware oder andere sicherheitsrelevante externe Produkte oder Dienste.

Eine herkömmliche Anwendungssicherheit baut Schutzebenen direkt in die Anwendung selbst ein. Wie Anti-Malware-Anwendungen im PC ist die Anwendungssicherheit die absolut letzte Verteidigungslinie für serverbasierte Anwendungen. Wenn ein Angriff so weit vordringt konnte, dann ist auf dem Weg dahin bei der Informationssicherheit etwas katastrophal falsch gelaufen.

Defense-in-Depth

Kein einzelner Anbieter kann ein Netzwerk vor heutigen Bedrohungen bewahren. Auch verfügt niemand über genügend Personal oder Forschungs- und Entwicklungskapazitäten, um ausreichend schnell innovative neue Konzepte zur Abwehr aufkommender Bedrohungen bereitzustellen.

Der einzig realistische Weg, ein modernes Netzwerk zu verteidigen, besteht darin, dass mehrere Produkte verschiedener Anbieter eng zusammenwirken, um so einen mehrschichtigen, tiefgreifenden Schutz zu bieten.

Verschlüsselung und DLP

Verschlüsselung und Data Loss Prevention (DLP) sollen verhindern, dass Daten im Netzwerk nach außen gelangen.

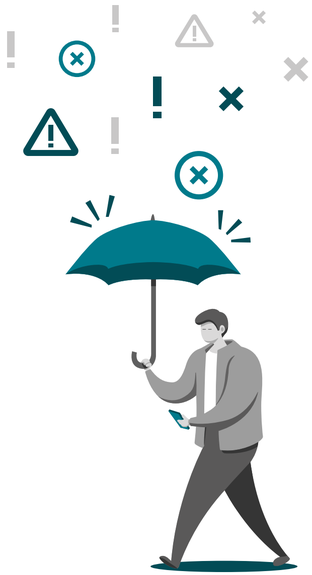
Verschlüsselungsverfahren sorgen dafür, dass nur Personen oder Anwendungen mit dem richtigen Schlüssel auf Daten zugreifen können.

Einem Unternehmen kann großer Schaden entstehen, wenn beispielsweise der Laptop eines Vertriebsleiters, komplett mit unverschlüsselten Kundendateien, gestohlen wird.

Durch die Verschlüsselung wird bei der Übertragung von Daten dafür gesorgt, dass diese nicht von Dritten ausspioniert werden können. Das ist von entscheidender Bedeutung für den Zugriff auf Dienste, die über das Internet bzw. über ein Funknetzwerk angeboten werden (weder das Internet noch Funknetzwerke können jemals 100%ig abgesichert werden).

Das grundlegende DLP-Konzept besteht darin, Daten, die das Netzwerk verlassen wollen, zu scannen und zu stoppen, falls diese Daten nicht abfließen dürfen. Es ist häufig Teil von NGFW- und NGAV, um beispielsweise zu verhindert, dass Dateien mit einer bestimmten Art von Inhalten auf Flash-Datenträger kopiert oder in einen Cloud-Datenspeicher (wie etwa Dropbox) hochgeladen werden können.

DLP ist oft in Sicherheitstools integriert, die CASBs (Cloud Access Security Brokers) und ATP-Produkte (Advanced Threat Protection) beinhalten, um zum Beispiel die Übertragung einer Tabelle mit Kreditkartendaten zu erkennen und einen Alarm oder eine Blockierung auszulösen.



Allerdings gibt es noch weit mehr Möglichkeiten, Daten aus einem Netzwerk zu schmuggeln: Instant Messenger, Slack und soziale Medien werden durch moderne DLP nur unzureichend abgedeckt.

Grundlegende InfoSec-Maßnahmen

Überwachung

Ohne Überwachung hätte IT-Personal keine Möglichkeit, zu erfahren, was geschieht oder auf welche Probleme reagiert werden muss. Die meisten Überwachungsprodukte erkennen Muster anhand von Abweichungen und Korrelation.

Abweichungen stützen sich auf die Beobachtung von Workloads und Datenströmen zwischen Systemen in Echtzeit, um eine Grundlage dafür zu ermitteln, was als „normal“ anzusehen ist und dann diese Abweichungen als Norm zu identifizieren.

Auf Korrelationen basierende Überwachung sucht nach mehreren gleichzeitig oder schnell nacheinander auftretenden Ereignissen, die auf ein Problem hinweisen und orientiert sich üblicherweise an den Ereignisprotokollen, die von Anwendungen oder Infrastrukturkomponenten generiert werden.

Das ideale auf Überwachung basierende DLP-System untersucht den Datenzugriff innerhalb der IT-Infrastruktur des gesamten Unternehmens und sucht nach Abnormitäten. Wenn dann zum Beispiel ein Vertriebsmanager, der normalerweise nur auf Daten von einigen wenigen Konten am Tag zugreift, plötzlich die Daten aller Kundenkonten in seiner Region abruft, erkennt das System, dass etwas Unerwartetes geschehen könnte. Dieses Konzept erfordert mehrere Produkte mehrerer Anbieter, die zusammenarbeiten.

Die vollständige Überwachung aller Daten eines Unternehmens ist jedoch oft nicht möglich. Unternehmen können Daten an Tausenden verschiedenen Standorten und Systemen gespeichert haben, sowohl hausintern als auch in der Public Cloud.

Selbst wenn ein Unternehmen alle Datenzugriffe überwachen könnte, bliebe die Frage, was geschehen solle: Wenn Zugriffsmuster von der Norm abweichen, könnte ein Mitarbeiter versuchen, Daten zu stehlen, es könnte sich um eine Gefährdung durch einen externen Hacker handeln oder einfach um jemanden, der seinen Job erledigen will. Zunehmend wird maschinelles Lernen zur Optimierung dieser Muster eingesetzt, und in den kommenden Jahren dürfte es auf diesem Gebiet erhebliche Fortschritte geben.

SIEM und ATP

Produkte für Security Information und Event Management (SIEM) sind der Kern der InfoSec und zunehmend mit ATP-Produkten verwoben. Sie erhalten Daten von mehreren Produkten und die nützlichsten lassen sich schnell und unkompliziert in führende Produkte verschiedener Anbieter integrieren.

Bei den erfolgreichsten SIEMs und ATPs liegt der Schwerpunkt in der Korrelation. Hier ein Beispiel:

1. Die NGFW sendet E-Mail-Datenströme an die ATP, die eine Reihe von mit Malware verseuchten E-Mails an einen bestimmten Benutzer entdeckt.
2. Die ATP weist die Firewall an, die Zustellung der E-Mails zu verhindern.
3. Kurz danach erkennt die NGAV-Funktion im Endgerät des betreffenden Benutzers seltsames Verhalten.
4. Der CASB erkennt, dass das Endgerät versucht, eine Verbindung zu Cloud-Datenspeicher-Websites aufzubauen und Dokumente hochzuladen.

Während der Schweregrad der Warnmeldung für jedes einzelne der Ereignisse wahrscheinlich gering sein wird, kann die ATP-Funktion durch Korrelation der Ereignisse feststellen, dass wahrscheinlich ein gezielter Angriff stattfindet, diesen als maximale Bedrohung definieren und einen Zuständigen alarmieren.

SIEMs erfassen vor allem Ereignis- und Überwachungsdaten und viele Anbieter erweitern die Lösungen inzwischen mit Scanfunktionen, bauen DLP ein oder ermöglichen die Integration in eine Anwendung mit DLP.

Grundlegende InfoSec-Maßnahmen

Zugriffskontrolle, VPN und Fernzugriff

Dank InfoSec-Techniken wie der Verschlüsselung ist es möglich, zwar physischen Zugriff auf einen Datenspeicher, aber keinen Zugriff auf die tatsächlichen Daten zu haben. Ebenso kann Cloud Computing Unternehmen den Zugriff auf Produkte, Dienste und Daten von überall aus gestatten, ohne jemals auf die zugrunde liegende Hardware zugreifen zu können.

Für praktisch jeden Teil der IT-Infrastruktur sowie das Betriebssystem und die Anwendungen gibt es eine Art Zugangskontrolle. Zu den beiden wichtigsten Methoden der Zugriffssteuerung gehören Virtual Private Networks (VPNs) und den Fernzugriff.

VPNs sind verschlüsselte Netzwerktunnel zwischen zwei Computersystemen. Sie werden verwendet, um Einzelnen den Aufbau sicherer Verbindungen zum internen Netzwerk ihres Unternehmens zu ermöglichen und sichere Verbindungen zwischen Standorten einzurichten. Außerdem nutzen sie Verschlüsselung zum Schutz vor Snooping durch böswillige Akteure.

Fernzugriff oder Remote-Zugriff bezeichnet Technologien, die es Einzelnen ermöglichen, ohne Einsatz von VPNs auf Unternehmensressourcen zuzugreifen.

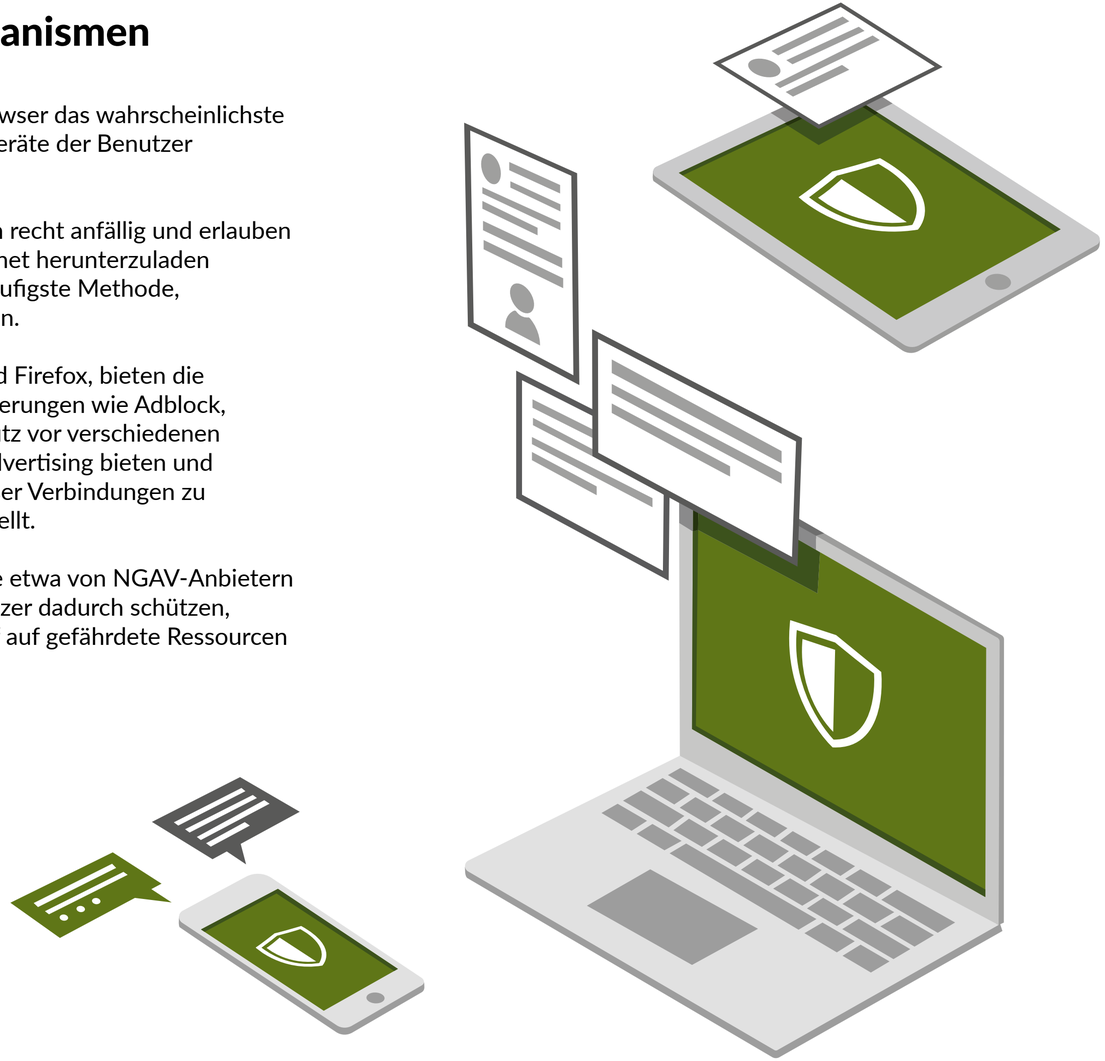
Browser-Abwehrmechanismen

Neben E-Mail sind vermutlich Webbrowser das wahrscheinlichste Einfallstor für externe Angreifer, um Geräte der Benutzer bzw. Endpunkte zu gefährden.

Aktuelle Webbrowser sind immer noch recht anfällig und erlauben den Benutzern, Dateien aus dem Internet herunterzuladen und sie dann auszuführen – die dritthäufigste Methode, die Informationssicherheit zu gefährden.

Beliebte Webbrowser, wie Chrome und Firefox, bieten die Möglichkeit zur Installation von Erweiterungen wie Adblock, Ghostery und Privacy Badger, die Schutz vor verschiedenen Formen von Internet-Attacken wie Malvertising bieten und vermeiden wollen, dass der Webbrowser Verbindungen zu verdächtigen Internetressourcen herstellt.

Andere Browsererweiterungen, wie sie etwa von NGAV-Anbietern bereitgestellt werden, sollen Endbenutzer dadurch schützen, dass sie Anforderungen für den Zugriff auf gefährdete Ressourcen nicht ausführen.



Grundlegende InfoSec-Maßnahmen

MDM

Produkte für Mobile Device Management (MDM) sind für Geräte vorgesehen, die außerhalb der Grenzen des Unternehmens genutzt werden, wie Handys, Tablets und Laptops. Sie wenden bei Geräten für Telearbeit und Mobilgeräten sicherheitsspezifische Vorlagen, Profile und Richtlinien an und stellen sicher, dass diese Geräte die Anforderungen des Unternehmens an die Informationssicherheit erfüllen, bevor sie eine Verbindung zu Ressourcen innerhalb des Unternehmensbereichs herstellen können.

MDM ermöglicht die sichere Bereitstellung von Anwendungen über Lösungen wie App-Stores und Virtual Desktop Infrastructure (VDI). MDM-Produkte kümmern sich auch um die Zugriffssteuerung und stellen sicher, dass nur der autorisierte Benutzer das Gerät verwenden kann. Außerdem ermöglichen sie bei Diebstahl oder anderweitigem Verlust die Nachverfolgung und die ferngesteuerte Löschung.

Authentifizierung

Die Technologien für die zentralisierte Authentifizierung und Unified Authentication (UA) stützen sich auf Verzeichnisdienste wie LDAP, SAML oder Active Directory von Microsoft. Single Sign-On (SSO) ist die bekannteste UA-Technologie. Sie zielt darauf ab, dem Benutzer mit einem einzigen Benutzernamen und Passwort den Zugang zu Workloads und Diensten mehrerer Anbieter zu ermöglichen, die auf mehreren unterschiedlichen Infrastrukturen bereitgestellt werden.

Systeme für Multi-Faktor-Authentifizierung (MFA) sind ebenfalls weit verbreitet, können jedoch Komplikationen verursachen, wenn sie sich möglicherweise je nach Land unterscheiden müssen. So müssen Benutzer zum Beispiel bei einer SMS-Verifizierung (einem allgemein üblichen MFA-Konzept) einen Code aus einer Textnachricht eingeben, um sich anzumelden. In vielen Ländern gibt es jedoch Beschränkungen für SMS-Nachrichten, die diese Methode unzuverlässig machen können oder es sind zusätzliche Integrationen notwendig, damit sie korrekt funktioniert.

Automatisierung

Die Anzahl und Vielfalt der verwalteten Workloads nimmt rasant zu. Das Tempo, in dem sich die IT verändert, hat sich seit längerer Zeit ständig erhöht und die Menschen können ohne Hilfe nicht mithalten. Hier setzt die Automatisierung an.

Automatisierung ist die weitaus wichtigste Maßnahme für die Informationssicherheit.

Aufgrund der starken Vernetzung der heutigen IT-Umgebung, der sich schnell auflösenden Grenzen von Netzwerken und der Tatsache, dass Bedrohungen auch hinter der Abgrenzung lauern, muss die Informationssicherheit Bestandteil aller Bereiche der IT sein. Jeder Teil der IT-Infrastruktur, jede Workload und jedes mit dem Netzwerk verbundene Gerät muss in die InfoSec-Planung eines Unternehmens einbezogen werden.

Anatomie eines Angriffs

Festlegen eines Ziels

Stellen Sie sich einen Hacker vor, wir nennen ihn Bob (es gibt natürlich auch Frauen unter den Hackern, aber statistisch sind die kriminellen eher männlich). Bobs Ziel ist PotatoCom, ein lokaler Anbieter von Internetdiensten. PotatoCom hat sich zum x-ten Mal geweigert, einen Glasfaser-Internetzugang zu installieren und Bob hat das schreckliche ADSL satt. Aus Rache will Bob das Finanzsystem von PotatoCom dadurch gefährden, dass er den Zugriff der Firma auf ihre eigene Datenbank sperrt.

Um sich die Kontrolle über das System zu verschaffen und seinen Plan umzusetzen, muss Bob kein Supertechnologe sein, sondern nur genug lernen, um sein Ziel zu erreichen.

Konnektivität

Bob muss einen Weg finden, seine illegalen Online-Aktionen so auszuführen, dass sie nicht auf ihn zurückgeführt werden können. Er könnte ein ungesichertes öffentliches WLAN in einem Café nutzen, müsste dabei aber darauf achten, nicht von Überwachungskameras erfasst zu werden, auch nicht von denen auf seinem Weg dorthin. Um sich zu schützen, falls er an einer Kamera vorbeikommt, die er nicht umgehen kann (oder die er nicht entdeckt hat), könnte er sich verkleiden.

Er verwendet nie zweimal denselben WLAN-Hotspot und wechselt die Art der Verkehrsmittel, die er auf dem Weg zu verschiedenen Orten mit kostenlosem WLAN nutzt, um ein erkennbares Muster seines Tuns zu vermeiden. Wenn Bob dem jeweiligen WLAN nahe genug kommt, muss er für die Netzwerkverbindung eventuell nicht einmal das Gebäude des Unternehmens mit dem kostenlosen WLAN betreten.

Außerdem muss Bob sein Tun vor den Überwachungstechnologien in den von ihm genutzten Netzwerken verbergen. Er wird wahrscheinlich ein VPN oder mehr als eines verwenden müssen. Weiterhin könnte er eine VM bzw. einen Server in einer virtuellen Maschine als Ausgangsort seiner Angriffe mieten. Um seinen Internet-Datenverkehr weiter zu verbergen, wird er vermutlich TOR, I2P oder eine andere Methode der Anonymisierung und Verschlüsselung wählen.

Bezahlung

Jedes Mal, wenn er online gehen will, muss Bob für USB-Flash-Datenträger, Notebooks, zwei Konten für VPN-Dienste und zwei private VM-Mieten bezahlen. Er muss sich also überlegen, wie er das bewerkstelligen kann, ohne identifiziert zu werden. Es gibt Möglichkeiten dafür – zwar auf Umwegen, aber es ist möglich. Um es kurz zu machen: Bob schafft es (auf legalem Weg), sein Bargeld in eine Prepaid-Kreditkarte umzuwandeln, die er überall verwenden kann und die keine Rückverfolgung zu ihm ermöglicht.

Forschung

Bob muss herausfinden, welche Datenbank und Backup-Systeme PotatoCom verwendet und wie man in die Systeme der Firma gelangen kann. Er kann technische Mittel einsetzen, um die IT-Infrastruktur von PotatoCom zu untersuchen. Er könnte mit Social-Engineering-Methoden Mitarbeiter von PotatoCom ansprechen, sich als sachkundig (oder Insider) ausgeben und den Betreffenden Gelegenheit geben, Dampf abzulassen, was meistens funktioniert. Er könnte auch in sozialen Medien finden, was er braucht, indem er nach PotatoCom-Mitarbeitern sucht, die sich über die von ihnen verwendeten Tools beschweren. Bob könnte sogar versuchen, den Support einiger Hersteller anzurufen und vorzugeben, er sei bei PotatoCom beschäftigt, nur um festzustellen, ob PotatoCom zu deren Kunden zählt.

Anatomie eines Angriffs

Eindringen in das System

Die einfachste Methode, sich Zugang zu einem System zu verschaffen, besteht darin, jemanden so psychologisch zu manipulieren, dass derjenige seine gültigen Zugangsdaten für das Einloggen preisgibt. Bob braucht keine Administrator-Zugangsdaten. – Ihm ist jeder recht, der die Infrastruktur sehen kann, selbst wenn derjenige keine Änderungen an der Infrastruktur vornehmen kann. Von dieser Position aus könnte er mit Netzwerkscans die Infrastruktur untersuchen und per „Lateral Movement“ weiche Ziele angreifen. Wenn es mehrere Hintertüren in das System gibt, könnte Bob mit technischen Mitteln versuchen, in die Datenbank vorzudringen und Datensätze zu beschädigen. Das wäre dann die eher schwierige Methode.

Alles was Bob eigentlich braucht, um die Sicherheitsvorkehrungen von PotatoCom zu überwinden, ist deren Administrator-Passwort.

Die Firma hat ihre gesamte Infrastruktur bei einem einzigen Cloud-Anbieter, da liegt es nahe, dass sie für die Administration eventuell dieselben Zugangsdaten verwendet wie für die Produktionsumgebung des Unternehmens und die Backups (keine sicherheitsbewusste Praxis, aber es kommt vor).

Das Ziel kennenlernen

Bob wird wahrscheinlich auch nicht mit sozialer Manipulation in der Lage sein, an jemanden mit Administrator-Zugangsdaten heranzukommen, da sich diese Mitarbeiter meist sicherheitsbewusster verhalten. Deshalb sucht er sich ein geeignetes Opfer aus und setzt physische Überwachungsmöglichkeiten ein.

Bob lernt mehr über sein Ziel und nutzt dieses Wissen, um die Schwachstelle zu finden, die ihm auf die eine oder andere Weise ermöglicht, an die gewünschten Administrator-Zugangsdaten zu kommen.

Beispielsweise sind Wohnungen nie so gut gesichert wie Büros und es gibt viele Möglichkeiten, Menschen in ihrer eigenen Wohnung auszuspionieren. Wenn die Zielperson nicht von zu Hause aus arbeitet, wo befindet sich ihr Büro? Bob könnte sich, wieder per Social Engineering, Zugang zum Büro verschaffen und eine Kamera oder einen Keylogger anbringen, durch Fenster spähen oder Signale einer Funktastatur abfangen.

Denken wie ein Hacker

Nachdem er eine Verbindung zur Infrastruktur von PotatoCom hergestellt hat, deaktiviert Bob Funktionen für Änderungsberichte und beschädigt die Datenbank. Dann erstellt er ein Backup der Datenbank und löscht ältere Backups, ändert das Passwort von PotatoCom und vernichtet alle Indizien.

Die Finanzdatenbank von PotatoCom ist jetzt unbrauchbar und die Firma kann nicht auf ihr Benutzerkonto zugreifen, um herauszufinden, was passiert ist. Sie ist nicht mehr in der Lage, Kunden eine Rechnung zu stellen, Lieferanten zu bezahlen oder Steuererklärungen abzugeben. Es kann zu einer Betriebsprüfung kommen und die Firma gerät in Schwierigkeiten, weil sie keinen Zugriff auf die benötigten Daten hat. Möglicherweise muss sie sogar den Geschäftsbetrieb einstellen.

Nichts von dem, was Bob getan hat, war technisch besonders schwierig. Worauf es ankam, war die Denkweise. Bob hat große Anstrengungen unternommen, seine Identifizierung zu vermeiden. Und er suchte nach der einfachsten Methode, in das System einzudringen: Der am besten ausnutzbare Teil jedes Systems ist üblicherweise der Mensch, der dafür Verantwortung trägt. So denkt ein Hacker.

Um einen Hacker abzuwehren, braucht der dafür Zuständige nur die richtige Denkweise: Sicherheit geht vor.

Ein für die Sicherheit Verantwortlicher muss wie ein Hacker denken – nach ausnutzbaren Sicherheitslücken suchen – und diese mithilfe geeigneter Technologie, Geschäftsprozessen oder sogar einfach nur mit Vorhängen an Fenstern schließen. Verteidiger des Systems entdecken das dafür notwendige Werkzeug, sobald sie wissen, was sie verteidigen. Wie bei Hackern ist es die Denkweise, auf die es ankommt.

Weitergehende Konzepte

Einhaltung gesetzlicher Vorschriften

In zunehmendem Maße reicht es nicht mehr aus, einfach Technologien für die Informationssicherheit zu implementieren oder Audits zu bestehen, indem man IT-Richtlinien nach dem Kästchenprinzip anwendet. Unternehmen bzw. Organisationen sind aufgefordert, darzulegen, dass sie die Grundlagen und Ursachen für die Notwendigkeit der Informationssicherheit wirklich verstanden haben.

Die Datenschutz-Grundverordnung (DSGVO) der Europäischen Union (EU) macht es beispielsweise erforderlich, dass alle Unternehmen, die in großem Umfang mit Daten umgehen, einen Data Protection Officer (DPO) haben. DPOs sind dafür verantwortlich, dass ihre Unternehmen die DSGVO einhalten und es hat persönliche und erhebliche finanzielle Folgen, wenn der DPO oder das Unternehmen, für das er tätig ist, fahrlässig mit der Sicherung der Daten von EU-Bürgern umgeht.

Segmentierung und Mikrosegmentierung

Netzwerkadministratoren verwenden Segmentierung und Mikrosegmentierung, um zu verhindern, dass sich Angreifer, die es geschafft haben, hinter die geschützte Netzwerkgrenze vorzudringen, im Netzwerk ausbreiten („Lateral Movement“). Für jedes Segment (oder Mikrosegment, das nur eine einzige Anwendung beinhaltet) werden separate Schutzmaßnahmen getroffen. Diese Art der getrennten Absicherung schützt davor, dass sich Angriffe ungehindert im Netzwerk ausbreiten können, was besonders in gemeinsam genutzten Umgebungen wie bei Cloud-Service-Providern wichtig ist, wo IT-Infrastrukturen für mehrere Mandanten bereitgestellt werden.

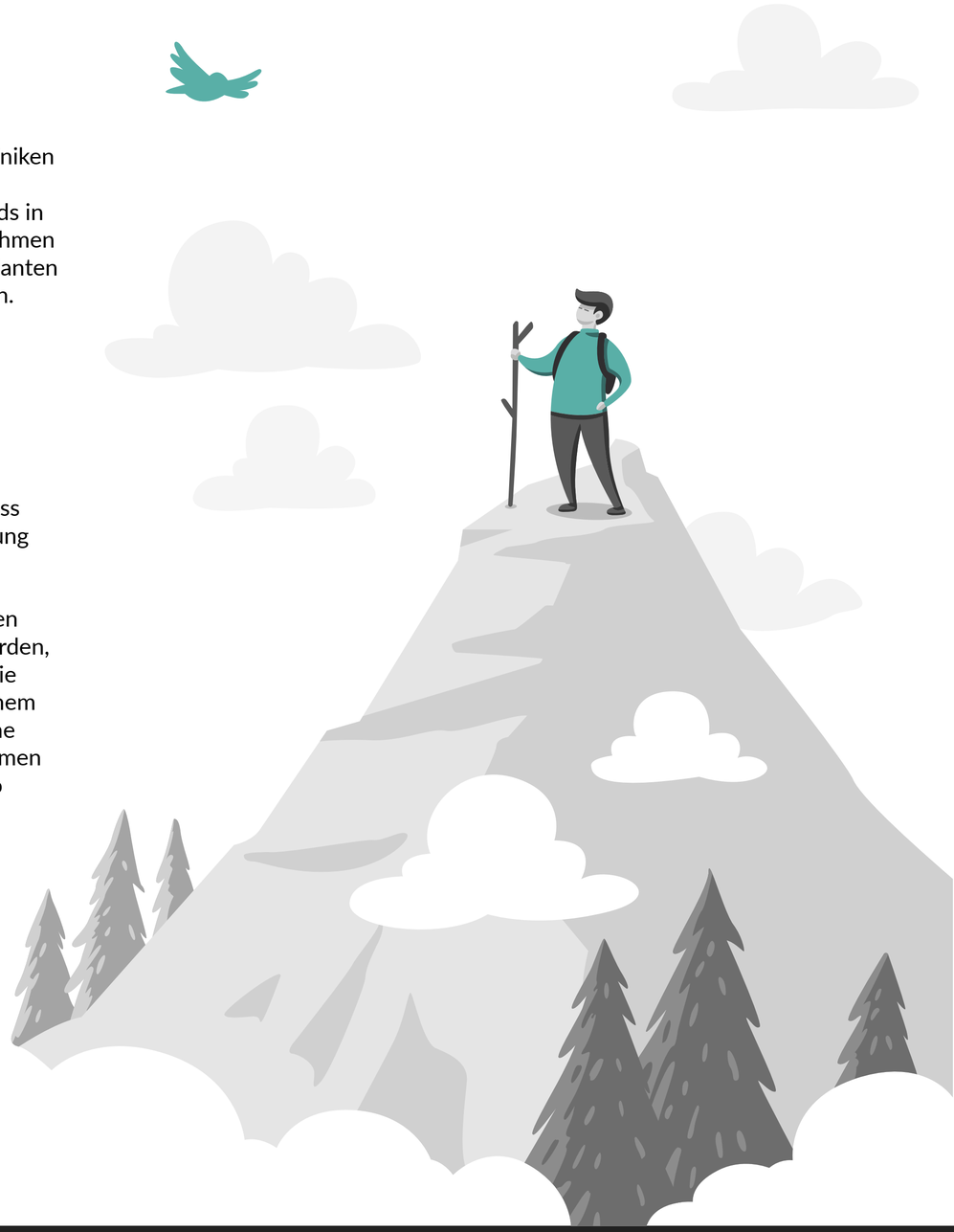
Die Mikrosegmentierung wäre beispielsweise in Forschungskliniken von Vorteil. Statt für jedes Forschungsprojekt eine eigene IT-Infrastruktur anschaffen zu müssen, können mit privaten Clouds in Kombination mit Mikrosegmentierung und geeigneten Maßnahmen für die Informationssicherheit die einzelnen Projekte als Mandanten auf der gemeinsamen IT-Infrastruktur der Klinik isoliert werden.

Fazit

Ereignisse, bei denen die Informationssicherheit (InfoSec) gefährdet wird, gehören zum IT-Alltag. Dass Vorgänge, die IT-Systeme gefährden, unvermeidbar sind, bedeutet nicht, dass Präventionsmaßnahmen unwirksam sind, aber es bedeutet, dass Unternehmen bzw. Organisationen für den Fall einer Gefährdung planen müssen.

In Verbindung mit Technologien für die Erkennung von Vorfällen und deren Eindämmung kann die Automatisierung genutzt werden, um Schritte zur Eindämmung eines Angriffs auszulösen, z. B. die Anforderung an einen Netzwerk-Switch, die Verbindung zu einem gefährdeten Gerät zu trennen oder das Gerät unter Quarantäne zu stellen. Das verhindert die Ausbreitung und kann Unternehmen unter Umständen zig oder sogar hunderte Millionen Dollar pro Ereignis ersparen.

Vorbeugung, Erkennung, Eindämmung von Vorfällen und die geeignete Reaktion sind die vier Bereiche der InfoSec-Verantwortlichkeit, denen sich die Unternehmen und Organisationen widmen müssen, wobei stets zu bedenken ist, dass es bei der Informationssicherheit auf der grundlegendsten Ebene immer um die Denkweise geht.



Juniper Connected Security

Sicherheit muss mehrschichtig sein

Die Verteidigung heutiger Netzwerke bedeutet die Verteidigung von allem in diesen Netzwerken und dies erfordert ein anderes Konzept für die Informationssicherheit, als es in den meisten Unternehmen umgesetzt wird.

Netzwerkbetrieb und Sicherheit sind eng miteinander verknüpft und wenn Verantwortliche versuchen, ihre Netzwerke mit Punktlösungen zu realisieren, kann dies verhängnisvolle Folgen haben. Wirksame Netzwerksicherheit entsteht durch die Zusammenführung mehrerer Sicherheitsebenen unter Einsatz verschiedener Technologien verschiedener Anbieter.

Switches, Router und WLAN-Access Points sind an Juniper Connected Security beteiligt und bieten umfassende Netzwerktransparenz und Ansatzpunkte für die Durchsetzung von Netzwerkrichtlinien – alles mit zentraler Automation und Orchestrierung. Dadurch profitieren Unternehmen von einem ausgedehnten Schutz, der anderweitig schwierig zu erreichen wäre.

Auch wenn Analytiker möglicherweise darauf hinweisen, die beste Lösung für ein bestimmtes Segment sei wahrscheinlich eine, die von einem Spezialisten für genau diesen Zweck käme, müssten Unternehmen bei einem solchen Konzept mehrere Produkte einsetzen und dann dafür sorgen, dass alle verschiedenen Teile harmonisch zusammenarbeiten. Dies kann die Automatisierung und Orchestrierung von Schutzmaßnahmen für das Netzwerk erschweren: Rangordnungen ändern sich laufend und die Umsetzung einer Automatisierung übersteigt oftmals die Lebenszyklen der Produkte, die automatisiert werden sollen.

Viele Anbieter haben ein vielfältiges Portfolio an Netzwerk- und InfoSec-Produkten, einschließlich Partner-Ökosystemen. Auch gibt es viele andere, die – wie Juniper – Kunden unterstützen, die in der Größenordnung von Service Providern tätig sind und die mit den ungewöhnlichsten, völlig überdimensionierten Netzwerken umgehen können, die sich Unternehmenskunden vorstellen können.

Was Juniper von anderen unterscheidet, ist das „connected“ in **Juniper Connected Security:** unser Engagement für Interkonnektivität. Juniper setzt sich für Integration und Orchestrierung ein, fördert die Verwendung offener Standards, offener Protokolle und offener APIs und unterstützt sogar konkurrierende Produkte. Es ist unser Ziel, Kunden dabei zu unterstützen, bereits vorhandene Einrichtungen und Geräte bestmöglich zu nutzen, anstatt von ihnen zu verlangen, dass sie diese ausmustern und ersetzen.

Dass im gesamten Portfolio von Juniper ein und dasselbe Betriebssystem – Junos – Verwendung findet, vereinfacht das zentralisierte Management erheblich und ermöglicht es Juniper, Managementplattformen mit umfangreicher Funktionalität anzubieten, mit lokalen oder Cloud-basierten Verwaltungsplänen oder einer Kombination von beiden. Junos OS macht die Erweiterung der Funktionalität im gesamten Portfolio wirtschaftlich.

Juniper Connected Security bietet Unternehmen die Möglichkeit, Benutzer, Anwendungen und die Infrastruktur dadurch zu schützen, dass die Sicherheit auf alle Verbindungspunkte im gesamten Netzwerk ausgedehnt werden. Die Durchsetzung einer Richtlinie, die einer Bedrohung so nahe wie möglich kommt, verringert das Risiko, dass diese Bedrohung sich weiter ausdehnt. Auch wird durch den Einsatz von maschinellem Lernen, Advanced Analytics und Automatisierung die schnelle Reaktion auf Vorfälle zur Realität.

Erfahren Sie mehr über Juniper Connected Security in Aktion.

Jetzt lesen

Lesen Sie hier das vollständige Buch „Basics of Cybersecurity“

Juniper Networks | Engineering Simplicity

PN: 7400127-001-DE

Unternehmens- und Vertriebshauptsitz
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Tel.: 888 JUNIPER (888-586-4737)
oder +1-408-745-2000
Fax: +1-408-745-2100
www.juniper.net/de

Hauptniederlassung für die Regionen APAC und EMEA
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, Niederlande
Telefon: +31-0207-125-700
Fax: +31-0207-125-701

Copyright 2020 Juniper Networks, Inc. Alle Rechte vorbehalten. Juniper Networks, das Juniper Networks Logo, Juniper, Junos und andere hier aufgeführte Marken sind eingetragene Marken von Juniper Networks, Inc. und/oder seinen angeschlossenen Unternehmen in den USA und anderen Ländern. Andere Namen sind möglicherweise Marken ihrer jeweiligen Eigentümer. Eine Haftung durch Juniper Networks für fehlerhafte Angaben in diesem Dokument wird ausgeschlossen. Juniper Networks behält sich das Recht vor, diese Veröffentlichung ohne Ankündigung zu ändern, zu übertragen oder anderweitig zu überarbeiten.