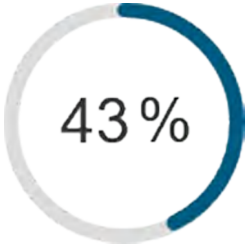
Sicherheitsgrundlagen für KMU

Gehen Sie das Thema Sicherheit vorausschauend an

Erfahren Sie, wie die Cyberbedrohungslandschaft für KMU heute aussieht, damit Ihr Unternehmen Angriffe überstehen, Betriebskosten senken und sicher wachsen, Sicherheit zur Priorität für alle machen und sich mit Cisco schützen kann.

Ihr Unternehmen wächst und es erregt Aufmerksamkeit. Diese ist aber nicht immer willkommen. Immer mehr raffinierte kriminellen Banden machen KMU zur Zielscheibe.



43 %

der Cyber-Angriffe richten sich gegen kleine Unternehmen. [1]

60 %

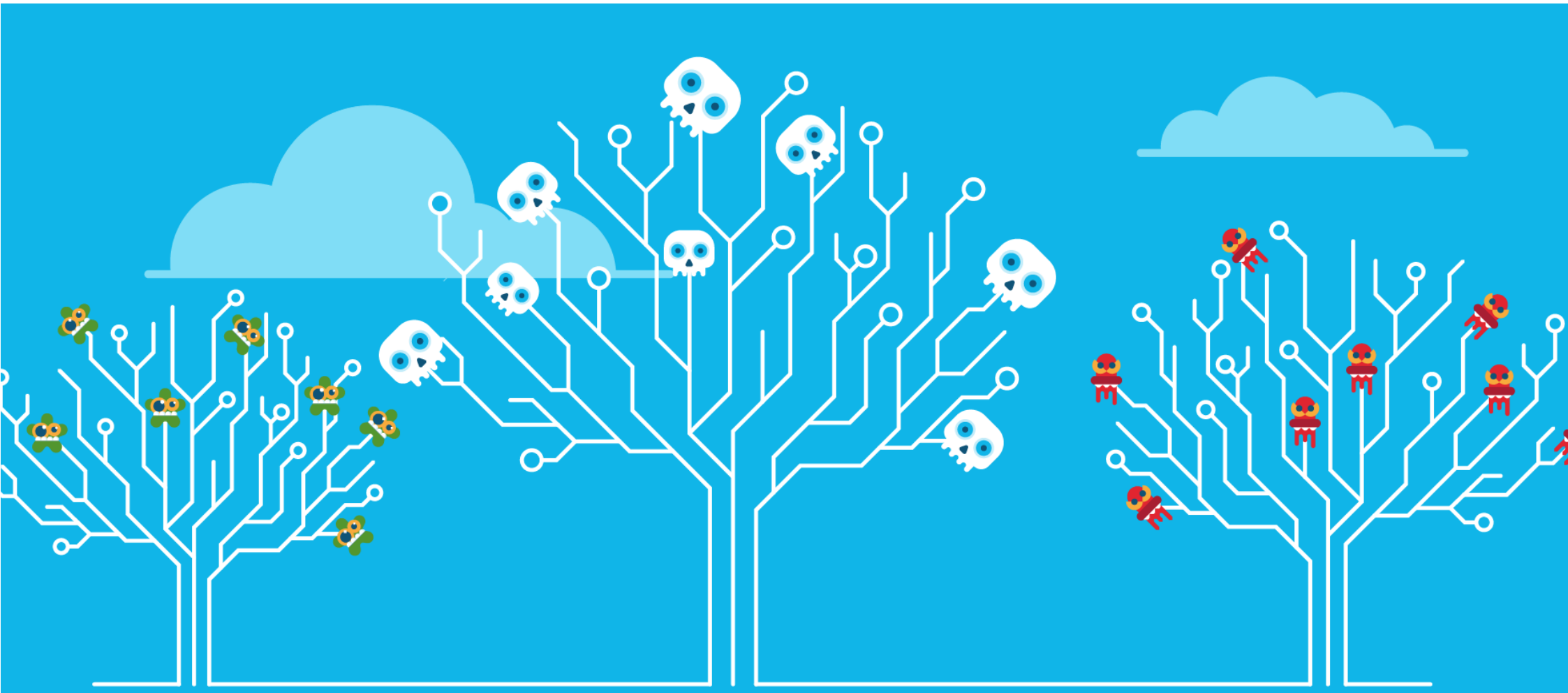
werden demzufolge schließen müssen. [1]

Cisco Annual Cybersecurity Report 2018 „Cisco ACR 2018“

2.235.018 USD pro Jahr

Der durchschnittliche Wert, den KMU infolge eines Cyber-Angriffs oder einer Datensicherheitsverletzung ausgegeben haben, weil IT-Ressourcen beschädigt oder gestohlen und der normale Betrieb gestört wurden.

Die traurige Wahrheit ist, dass das Überleben Ihres Unternehmens vom Verständnis der Cyber-Security abhängt.



Bedrohungen werden immer raffinierter

Hacker kennen Ihre Schwachstellen und nutzen Sie aus

Die heutzutage aktiven Hacker führen Angriffe nicht aus Spaß oder als Mutprobe durch. Die meisten tun es des Geldes wegen, sind gut organisiert und arbeiten selten allein. Angreifer sind flexibel, Unternehmen hingegen sind es nicht. Insbesondere dann, wenn sie das Thema Sicherheit nicht allzu ernst nehmen.

Das Ziel eines Hackers ist es, Kreditkarteninformationen, E-Mail-Adressen, Benutzernamen und Kennwörter zu stehlen. Einfach alles, was sich an den höher Bietenden verkaufen lässt. *Dabei* wenden sie einige der folgenden Methoden an.

Ransomware

Angreifer können Unternehmen mit Ransomware virtuell in Geiselhaft nehmen, was eine skrupellose Praxis ist. Ransomware verschlüsselt Ihre Dateien aus der Ferne und ohne Ihre Zustimmung. Einige Arten von Ransomware sind so programmiert, dass sie sich auch über das Netzwerk verbreiten.

Diese brauchen keinen Empfänger, der einen E-Mail-Anhang öffnet oder auf einen Link klickt. Aktuelle Ransomware wie WannaCry, die im Mai 2017 in Umlauf kam, sorgt dafür, dass Schadcode ohne Benutzereingriff zwischen Netzwerken übertragen wird. „WannaCry ist die erste Ransomware, die vollständig automatisiert ist“, erklärt Craig Williams, Senior Security Outreach Manager bei Talos, dem Sicherheitsforschungsbereich von Cisco.

WannaCry beeinträchtigte weltweit mehr als 200.000 Computer und wird wahrscheinlich Verluste von etwa 4 Milliarden US-Dollar verursachen. WannaCry wird über eine Schwachstelle im Microsoft KMU-Protokoll installiert und ist insbesondere in älteren Windows-Umgebungen wie Windows XP, Windows Server 2003 und Windows 8 effektiv. Microsoft hatte bereits eine Sicherheitsaktualisierung veröffentlicht, um diese Schwachstelle zu reparieren, es wurden aber nicht alle Benutzer automatisch geschützt.

Lösegeld von KMU gefordert

52 Prozent der KMU, die für den Bericht des Ponemon Institute von 2017 zur Situation der Cybersicherheit in kleinen und mittelständischen Unternehmen (KMU) befragt wurden, hatten im Zeitraum von 12 Monaten mit einem erfolgreichen oder erfolglosen Ransomware-Angriff zu kämpfen. Sobald die Infizierung abgeschlossen ist, erscheint eine Nachricht auf dem Bildschirm, in der ein Lösegeld in Bitcoins für die Freigabe Ihrer Daten gefordert wird. Eine typische Lösegeldsumme kann zwischen 200 und 10.000 GBP betragen, aber einige Unternehmen bezahlten am Ende weitaus mehr.
Kürzliche Schlagzeilen zeigen, dass sich eine neue Generation von Bedrohungen auf globaler Ebene schneller als je zuvor ausbreitet. Die Cisco Talos-Bedrohungsforschungsgruppe hat eine

Bedrohung namens VPNFilter entdeckt, die weltweit über 500.000 kleine Büro/Home-Office-Router und NAS-Geräte kompromittierte. Cisco Geräte waren davon nicht betroffen. Diese komplexe Bedrohung erlaubt dem Angreifer, den Datenverkehr durch die Geräte zu beobachten, Dateien von Backup-Laufwerken im Netzwerk zu stehlen und sich womöglich in verbundene Unternehmensnetzwerke einzuklinken.

Cyber-Kriminelle kennen ihre Ziele in und auswendig und wissen sogar über deren Vorlieben, Abneigungen und geschäftlichen Aktivitäten Bescheid. Sie wissen, was Unternehmen für die Freigabe ihrer Daten zahlen können, und sind in der Lage, Schwachstellen rücksichtlos auszunutzen.

Business Email Compromise (BEC)

Business Email Compromises (BEC) sind zu 75 Prozent rentabler als Ransomware. Nichtsdestotrotz erreichen sie keinen so großen Bekanntheitsgrad.

BEC sind gezielte Angriffe, für die Hacker Social Engineering anwenden und Menschen manipulieren, ihnen Geld zu überweisen. Es gibt keine Malware und keine Anhänge. Anders als beim Ransomware-Angriff werden Opfern keine Daten gestohlen. Alles basiert auf Lügen und Irreführung.

In der Regel verbringen Hacker einige Zeit damit, das ausgewählte Unternehmen zu recherchieren und ein Profil zu erstellen. Wenn sie ausreichend Informationen gesammelt haben, senden sie eventuell Spear-Phishing-E-Mails an leitende Mitarbeiter, die häufig in der Finanzabteilung arbeiten. Dabei muss es sich um eine Person handeln, die Geldüberweisungen tätigen darf. Je größer das Unternehmen, desto mehr Geld können sie herausschlagen. Allerdings nehmen Angriffe auf kleine und mittelständische Unternehmen zu.

Je größer das Unternehmen, desto mehr Geld können sie herausschlagen. Allerdings nehmen Angriffe auf kleine und mittelständische Unternehmen zu.

Datensicherheitsverletzung

Daten sind das Kernstück aller Unternehmensaktivitäten: Sie sind Ihr geistiges Eigentum, Ihre nächste große Chance, Ihre Kundendaten und Ihr Umsatz. Eine Sicherheitsverletzung kostet wesentlich mehr als die Behebung von Störungen und die Reparatur von beschädigten Systemen.

Der Aufbau eines starken Sicherheitsstatus kann dabei helfen, Ihr geistiges Eigentum und Ihren Ruf zu schützen. Im Durchschnitt brauchen Organisationen 191 Tage, um eine Sicherheitsverletzung zu erkennen und 66 Tage, um sie einzudämmen. (Quelle: Ponemon Institute) Doch der Schlüssel zur Schadensbegrenzung ist eine frühzeitige Erkennung.

Bei Cisco beträgt der Median für die Erkennung 3,5 Stunden. Wenn eine Sicherheitsverletzung eintritt, sind die Experten der Cisco Incident Response Services innerhalb von Stunden zur Stelle, um Ihnen dabei zu helfen, sie einzugrenzen und die Ursache zu beheben.

Angriffe auf die Lieferkette

Angriffe auf die Lieferkette sind eine neue und wachsende Cyberbedrohung, die zeigt, wie geschickt Cyber-Kriminelle geworden sind. Dabei geschieht Folgendes: Die Angreifer kompromittieren die Software-Update-Mechanismen von (eigentlich legitimen) Softwarepaketen. Dies erlaubt ihnen, sich über die Verteilung der Original-Software heimlich Zutritt zu verschaffen.

Die Cyber-Kriminellen werden im Wesentlichen ein Unternehmen in der Lieferkette angreifen, das schwache Cybersicherheitsverfahren aufweist, vor allem, was den Austausch von Informationen angeht. Deshalb werden KMU häufig angegriffen.

Sobald er das schwache Glied in der Kette identifiziert hat, kann sich der Angreifer um die Ausbeutung des ultimativen, beabsichtigten Ziels konzentrieren.

Schutz gegen Angreifer überall

Lassen Sie nicht zu, dass Ihr Unternehmen von Angreifern gestört wird. Bekämpfen Sie sie überall dort, wo sie sich Zutritt verschaffen wollen. Unsere Lösungen schützen Sie von der DNS-Schicht über die E-Mail bis hin zum Endpunkt. Dahinter steht die branchenführende Bedrohungsforschung von Talos.

Was tun?

Fragen Sie Ihre Hersteller/Partner, wie sie ihre Lieferketten sichern, wenn Sie Teil einer Lieferkette sind. Befragen Sie sie zu ihren Entwicklungsverfahren und ihren internen Sicherheitskontrollen. Wie führen sie Patches und Updates für ihre internen Systeme durch und wie oft? Wie segmentieren und sichern sie ihre Entwicklung, Qualitätssicherung und Produktionsumgebungen? Wie überprüfen sie ihre Partner und Hersteller?

Und vergessen Sie auch nicht, all diese Fragen Ihrer eigenen Organisation zu stellen. Andernfalls könnten Sie feststellen, dass Ihre Organisation das schwächste Glied in der Lieferkette ist.

Weitere Informationen zu Angriffen gegen die Lieferkette: https://gblogs.cisco.com/uki/protecting-...

Zu viele Unternehmen haben ein „Stapelproblem“

In einigen Unternehmen gibt es schlicht keine klare Cybersicherheitsstrategie. Sie halten so lange an einer Lösung fest, bis diese zum Hindernis wird.

Andere versuchen, alle Eventualitäten abzudecken und haben am Ende ein Stapelproblem. Sie verfügen über punktuelle Sicherheitslösungen von unterschiedlichen Herstellern, die alle am selben Ort eingesetzt werden. Beide Umstände verheißen nichts Gutes.

Das Flickwerk aus nicht kompatibler Sicherheitstechnologie hinterlässt Lücken, verursacht Verwaltungsprobleme und Ineffizienzen, die Hacker nur zu gerne ausnutzen. Jede neue Sicherheitslösung bringt eine eigene Management-Oberfläche mit sich. Für jede neue Lösung wird Personal benötigt, entsteht Verwaltungsaufwand für die Einrichtung, müssen Richtlinien erstellt und auf Warnhinweise reagiert werden. Dabei ist nicht immer klar, ob sich dieser ganze Verwaltungsaufwand überhaupt lohnt, wo es doch anderweitig größere Probleme zu bewältigen gäbe.

Womöglich haben Sie nur die Komplexität erhöht, die Wirksamkeit insgesamt aber nur geringfügig gesteigert. Zudem wird Sicherheit immer noch vorrangig als IT-Problem betrachtet. Auch das macht die Situation nicht einfacher. Laut der Cisco Security Benchmarks Study sind einige Organisationen nicht der Ansicht, dass sich Geschäftsbereichsleiter mit dem Thema Sicherheit auseinandersetzen. Allzu oft sind sie der Meinung, dass sich die IT darum kümmern muss. Das ist ein echtes Problem, denn so werden Sicherheitslösungen nur notdürftig „aufgesetzt“ und nicht in das Unternehmenssystem integriert. Einsparungen führen nur zu Mehraufwand.

Wenn alles richtig läuft, können Sicherheitsbemühungen dem Unternehmen sogar förderlich sein und eine Plattform für Wachstum schaffen.

Die Angriffsfläche wird immer größer und komplexer

Wir arbeiten überall: zu Hause, im Büro, an Flughäfen, in Cafés. Doch herkömmliche Sicherheitslösungen schützen Mitarbeiter immer noch nur dann, wenn sie sich im Unternehmensnetzwerk befinden.

Die Ausgangssituation:

- Benutzer greifen mit ihren eigenen intelligenten Geräten von überall auf Ihr Netzwerk zu.

- Ihre geschäftlichen Anwendungen, Server und Daten befinden sich in der Cloud.

- Geräte, die nicht einmal mehr wie Computer aussehen, verbinden sich mit Ihren Netzwerken (z. B. intelligente Zähler, Thermostate, Drucker, Kameras usw.)

- Hinzu kommt, dass Sie nun herausfinden müssen, wie Sie die Sicherheit für diese komplexe Infrastruktur gewährleisten können.

Schatten-IT

Man spricht von Schatten-IT, wenn Mitarbeiter beliebige Anwendungen nutzen, die sie vorziehen, ohne dafür die Genehmigung der IT-Abteilung dafür einzuholen. Darunter fallen etwa Installationen von Sofortnachrichten-Programmen auf ein Unternehmensgerät oder das Herunterladen von Dateifreigabesoftware, die dann für die Übertragung vertraulicher Daten verwendet wird.

Die für den Bericht des Ponemon Institute von 2017 zur Situation der Cybersicherheit in kleinen und mittelständischen Unternehmen (KMU) befragten Unternehmen waren von einer Datensicherheitsverletzung betroffen. 54 Prozent gaben an, dass nachlässige Mitarbeiter daran schuld waren; das ist eine Zunahme um 48 Prozent im Vergleich zum Vorjahr.

Die Schatten-IT kann insbesondere dann riesige Sicherheitsschwachstellen verursachen, wenn Sie nicht wissen, wie weit das Problem reicht. Diese Vorgehensweise ist in etwa das Gleiche, wie wenn Sie in Fleisch gehüllt im Haifischgebiet schwimmen gingen. Trotzdem ist sie in Unternehmen weitverbreitet. Warum ist das so?

Fairerweise muss für die Mitarbeiter gesagt werden, dass sie es mit den besten Absichten tun. Sie möchten ihre eigene Produktivität verbessern und die neuesten digitalen Tools verwenden. Mitarbeiter denken dabei nicht immer an die Sicherheitsauswirkungen, wenn sie auf diese Anwendungen zugreifen. Manchmal verwenden Mitarbeiter Schatten-IT-Tools, weil sie für bestimmte Systeme in ihrer vorherigen Organisation verwendet wurden. Das ist schließlich einfacher, als etwas Neues zu lernen.

Beleuchtung der Schatten-IT

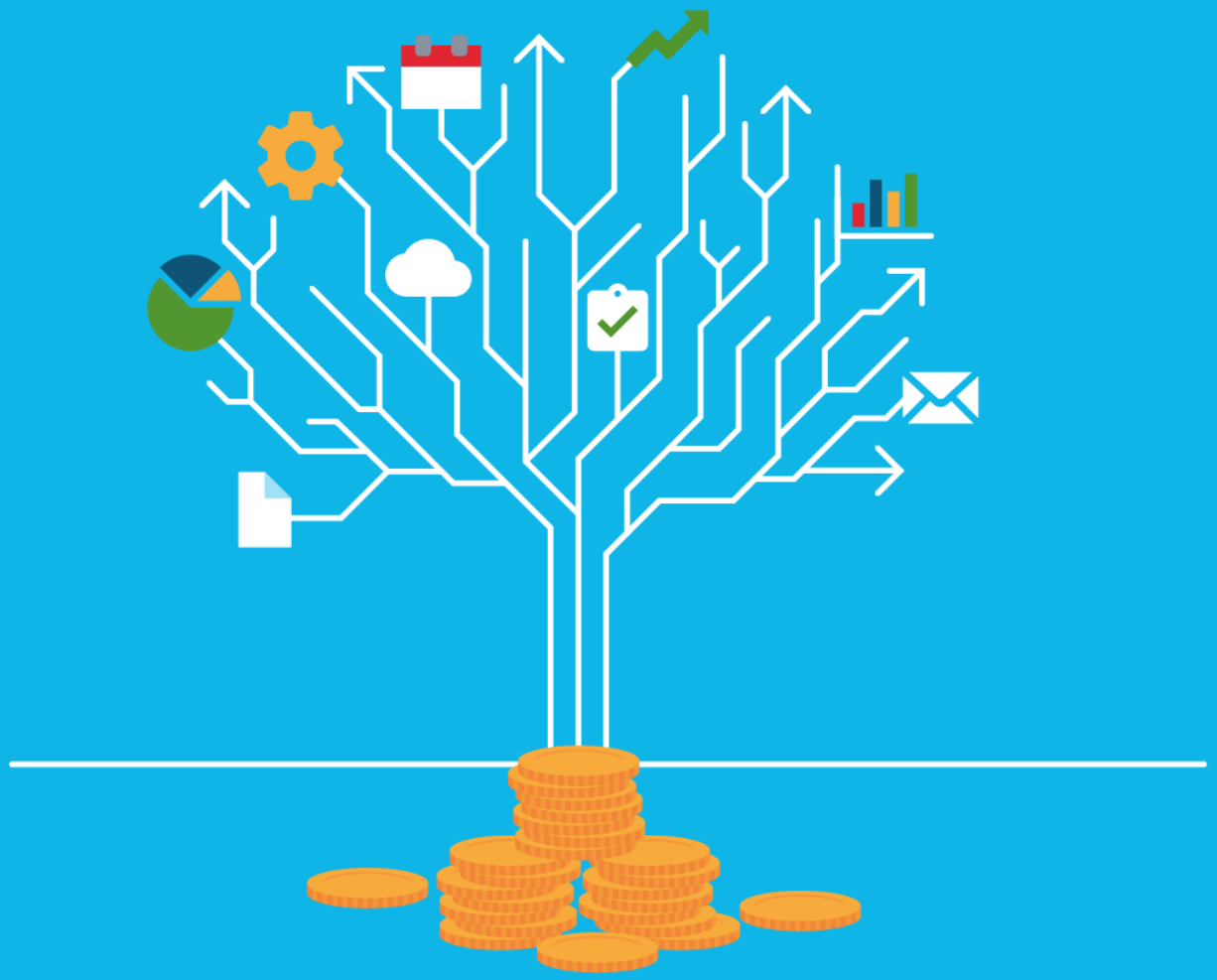
Es ist möglich, die Schatten-IT in einen positiven Beitrag für Ihr Unternehmen umzuwandeln:

- Wenn Sie es nicht bereits getan haben, richten Sie ein Forum oder Notiz-Tools ein, bei dem Ihre Mitarbeiter Ideen einreichen können, die den Geschäftsbetrieb verbessern könnten. Belohnen Sie Leute für ihre Beiträge und feiern Sie, wenn Ideen umgesetzt werden.
- Für eine effektive Sicherheit sorgt nicht nur die Technologie, es müssen auch geeignete Prozesse erstellt werden. Machen Sie das Thema Sicherheit zu einem wesentlichen Bestandteil Ihres Schulungsprogramms, damit Mitarbeiter verstehen, welche Konsequenzen die Verwendung von unsicheren Geräten und Programmen hat.
- Zu wissen, was in Ihrem Netzwerk vor sich geht, ist eine hohe Priorität der IT-Sicherheit. Leider wissen die meisten Unternehmen nicht, wann eine Sicherheitsverletzung stattgefunden hat, wie es dazu gekommen ist und wie groß der Schaden ist. Bauen Sie dem vor.

Kennwortrichtlinie

Starke Kennwörter spielen für die Cybersicherheit in KMU weiterhin eine wichtige Rolle. Trotzdem geben 59 Prozent der Befragten im aktuellen Ponemon-Bericht an – übrigens derselbe Prozentsatz wie im vorangegangenen Bericht –, dass sie keinen Überblick über die Kennwortpraktiken der Mitarbeiter haben und nicht wissen, ob sie schwer zu knackende oder starke Kennwörter nutzen.

Die Teilnehmer gaben außerdem an, dass Kennwortrichtlinien nicht strikt durchgesetzt werden. Wenn ein Unternehmen über eine Kennwortrichtlinie verfügt (bei 43 Prozent ist dies der Fall), sagen 68 Prozent, dass sie entweder nicht strikt durchgesetzt wird oder es nicht sicher ist, wie gut sie eingehalten wird.



Wachstum braucht Sicherheit

Eine schwache Cybersicherheit beeinträchtigt Innovation

Die Abwehr von Cyber-Angriffen ist sicherlich ein dringendes Anliegen, aber eine wesentlich beunruhigendere Folge einer schwachen Cybersicherheit ergibt sich aus deren Auswirkungen auf Wachstum und Innovation.

In einer kürzlich durchgeführten Studie von Cisco gaben beachtliche 71 Prozent der Führungskräfte an, dass Bedenken bezüglich der Cybersicherheit die Innovation in ihrem Unternehmen behindert hätten. Von den Befragten sagten 39 Prozent, dass sie geschäftskritische Initiativen aufgrund von Problemen mit der Cybersicherheit gestoppt hatten. Diese Antworten zeigen, wie Schwächen bei der Cybersicherheit die Fähigkeit der Unternehmen behindern, genau die Zeit für Innovationen zu nutzen, die sie benötigen würden, um sich im Wettbewerb durchzusetzen.

Digitalisierung, bahnbrechende und exponentielle Veränderung sind in einem wettbewerbsintensiven geschäftlichen Umfeld Normalität geworden. Flexible Unternehmen können sich einen deutlichen Vorsprung verschaffen, wenn sie Neues schaffen und schnell handeln können und experimentierfreudig sind.

Sicherheitsverletzungen beeinträchtigen nicht nur das Geschäftsergebnis

Wenn Sie Ihr Netzwerk nicht richtig schützen, kann dies weitreichende Konsequenzen haben, einschließlich Ausfallzeiten, Ausrüstungsschäden und -austausch, Reaktion auf Vorfälle, forensische Untersuchungen, interne Audits und Kommunikation.

Ein Verlust des Kundenvertrauens kann eine bisher starke Einnahmequelle dauerhaft schädigen. Wenn Sie Daten Ihrer Kunden verlieren, kann dies zu Klagen, Bußgeldern, zunehmender Regulierung und Kosten zur Behebung des Vorfalls führen. Und das ist noch lange nicht der gesamte Schaden. So geben Kunden möglicherweise nach einer Datensicherheitsverletzung im Einzelhandel nicht mehr gerne persönliche Informationen preis.

Ihr Unternehmen kann sich einen entscheidenden Vorteil verschaffen, wenn sie auf folgende Strategien setzen:

- Etablierte Technologien, wie Web, Mobilgeräte, Cloud, Ressourcenmanagement in Unternehmen und Customer Relationship Management

- Sich schnell entwickelnde Technologien wie künstliche Intelligenz und Datenanalytik

Diese Technologien helfen Unternehmen, leichter Zugang zu ihren Kunden zu finden, in neue Märkte einzusteigen und die Produktivität der Mitarbeiter zu verbessern. Gleichzeitig steigern sie Umsätze und senken Kosten. Cybersicherheitsbedenken können die Verfolgung einiger digitaler Geschäftsmodelle und Innovationen behindern.

Die Qual der Wahl

Viele Geschäftsleute stehen vor einem Dilemma. Entweder gehen sie das Risiko ein, etwas falsch

zu machen, oder sie werden von der Konkurrenz abgehängt. Sie glauben, dass sie weiter vorwärts drängen müssen, oder sie riskieren, von digitalen Innovatoren und anderen flexibleren Mitbewerbern überholt zu werden. In unserer Umfrage gaben 73 Prozent der Teilnehmer zu, neue Technologien und Geschäftsprozesse häufig trotz der damit verbundenen Cybersicherheitsrisiken einzuführen.

Unternehmen mit mangelnder Cybersicherheit befinden sich in einer denkbar schlechten Wettbewerbsposition: Sie hinken Mitbewerbern bei Innovationen hinterher, schützen sich jedoch gleichzeitig nicht ausreichend vor Cyber-Angriffen.

Wie würde sich eine Sicherheitsverletzung oder ein Ransomware-Angriff auf Ihr Unternehmen auswirken?

Was sind die möglichen finanziellen Auswirkungen eines Netzwerkausfalls infolge einer Sicherheitsverletzung oder der verwehrte Zugriff auf Daten nach einem Ransomware-Angriff?

- Könnte eine Sicherheitsverletzung oder ein Ransomware-Angriff die Lieferkette zum Erliegen bringen?
- Was würde passieren, wenn ein Angriff Ihre Website nicht mehr verfügbar macht?
- Verlässt sich Ihr Unternehmen auf E-Commerce-Funktionen auf seiner Website?
- Wie lange dürfte die Website offline sein, bis Ihr Unternehmen Verlust macht?
- Ist Ihr Unternehmen gegen Cyber-Angriffe oder gegen Missbrauch Ihrer Kundendaten versichert? Ist diese Versicherung ausreichend?
- Verfügt Ihr Unternehmen über Backup- und Recovery-Funktionen, um bei Bedarf Informationen nach einer Sicherheitsverletzung oder dem Verlust von Daten nach einem Ransomware-Angriff wiederherzustellen?

Wirtschaftspotenzial der Digitalisierung

Durch das Wirtschaftspotenzial der Digitalisierung lässt sich der Wert der Sicherheit bestimmen. Es basiert auf zwei Komponenten: zum einen auf völlig neuen Quellen zur Wertschöpfung, die sich aus Investitionen und Innovationen im Bereich der Digitalisierung ergeben, und zum anderen auf der Wertverschiebung in Unternehmen, die von ihren Fähigkeiten abhängt, digitale Funktionen zu nutzen.

Ein Teil des Wirtschaftspotenzials der Digitalisierung ist auf den defensiven Bereich der Cybersicherheit zurückzuführen, wie z. B.:

- Schutz des geistigen Eigentums
- Reduzierung von beschädigten Daten (sowohl interne als auch Kundendaten), Steigerung der Betriebszeit und Reduzierung von Netzwerkausfällen
- Schutz finanzieller Ressourcen
- Sicherung vertraulicher behördlicher, nationaler und politischer Informationen
- Wahrung des guten Unternehmensrufs

Erhalten Sie den kompletten Überblick. Lesen Sie den ultimativen Leitfaden über Cybersicherheit zur Steigerung der Profitabilität von Cisco.

Eine sichere Plattform für Wachstum

Mit der integrierten Sicherheitsarchitektur von Cisco können Unternehmen die Effektivität von Sicherheitslösungen verbessern, indem die Dauer bis zur Erkennung von Bedrohungen und zur Behebung des Vorfalls verkürzt wird. So können Kosten gespart (was den Kapitalaufwand und die Betriebskosten angeht) und die Produktivität der IT-Mitarbeiter gesteigert werden.

Ziehen Sie in Sachen Cybersicherheit alle am selben Strang

Machen Sie das Thema Sicherheit für alle zur Priorität

Manchmal braucht es einen entscheidenden Anlass, bis Cybersicherheitsinitiativen in Angriff genommen werden.

60 Prozent der KMU, die von einer Sicherheitsverletzung betroffen sind, müssen schließen. Das bedeutet vor allem für Sie Folgendes: Vorsicht ist besser als Nachsicht.

Stellen Sie die für Ihr Unternehmen spezifischen Risikofaktoren vor

Erläutern Sie dem Vorstand, welchen Sicherheitsbedrohungen Ihr Unternehmen im Speziellen ausgesetzt ist. Halten Sie sich nicht allzu lange mit allgemeinen Trends und Statistiken auf. Verdeutlichen Sie vielmehr, welche Verbindung zwischen diesen Sicherheitstrends und den für Ihr Unternehmen und Ihre Branche spezifischen Herausforderungen besteht. Je mehr Zusammenhänge Sie aufzeigen, umso klarer wird, wie wichtig dieses Thema ist.

Sie können mit der Unternehmensführung beispielsweise über die wichtigste Einnahmequelle des Unternehmens sprechen und in diesem Zusammenhang anhand von Beispielen erläutern, inwiefern Sicherheitsbedrohungen wie Ransomware eine Bedrohung darstellen können. Wenn in Ihrem Unternehmen vertrauliche Daten wie Finanzdaten gespeichert werden, können Sie anhand von Beispielen aufzeigen, welche rechtlichen Konsequenzen und Bußgelder Ihr Unternehmen zu erwarten hat, wenn diese Daten an die Öffentlichkeit gelangen.

Erläutern Sie, wie Angriffe funktionieren, wie einfach es sein kann, Sicherheitsbestimmungen zu verletzen. Nennen Sie konkrete Beispiele für Probleme, die sich Ihnen bereits stellen, und zeigen Sie auf, welche Risiken und langfristigen Konsequenzen sich aus diesen Problemen ergeben können.

Lassen Sie Zahlen sprechen.

Vorstände lieben Zahlen und Fakten. Daher sollten Sie Ihre Prioritäten in puncto Sicherheit unbedingt an den Zielen und Fristen Ihres Unternehmens orientieren. Berücksichtigen Sie die Unternehmens- und IT-Ziele, und zeigen Sie, wie diese mithilfe von Sicherheitsbestimmungen erreicht werden können.

Erläutern Sie aber auch, wie die Ziele durch einen Sicherheitsvorfall gefährdet werden können. Fragen Sie beispielsweise, welcher potenzielle Schaden für Ihr Unternehmen entsteht, wenn kurz vor der Einführung eines neuen Produkts geistiges Eigentum an die Öffentlichkeit gelangt oder vernichtet wird.

Und dabei muss es sich nicht einmal um eine hypothetische Frage handeln. Wenn Sie die Kosten beziffern können, die Ihrem Unternehmen bereits jetzt aufgrund von Sicherheitsproblemen entstehen, ist das ein noch besseres Argument.

Wiederholung ist wichtig.

Es ist unwahrscheinlich, dass Sie alle Ihre Forderungen in nur einem Gespräch durchsetzen. Führen Sie daher regelmäßig Gespräche, und kommunizieren Sie einfache Botschaften. Etablieren Sie regelmäßige Zusammenkünfte, und berichten Sie häufig über wichtige Kennzahlen. Scheuen Sie sich nicht, sich zu wiederholen. Legen Sie die Dinge aus unterschiedlichen Blickwinkeln dar, bis Ihre Botschaft verstanden wird, und sichern Sie sich die Geldmittel und die Unterstützung, die Sie benötigen.

Inwiefern fördert die DSGVO diesen Prozess?

Häufig tun sich Sicherheitsexperten schwer, dieselbe Sprache wie die Geschäftsführung zu sprechen und die Gründe dafür verständlich zu machen, warum Investitionen in die Sicherheit eine höhere Priorität eingeräumt werden muss. Wenn dann ein öffentlicher Cyber-Angriff stattfindet und die Unternehmensführung erkennt, welcher mehrdimensionale Schaden damit angerichtet wurde, liegen die Gründe für diese Investitionen plötzlich klar auf der Hand. Gespräche (und Veränderungen) sind viel schneller möglich, wenn das Problem erkannt wird.

An diesem Punkt können Gesetze wie die Datenschutz-Grundverordnung (DSGVO), die im Mai 2018 in Kraft trat, zu mehr Sicherheit beitragen.

Unternehmen, die bereits in die Sicherheit investieren, werden sich wohl keine großen Sorgen machen müssen, da sie wahrscheinlich auf dem besten Weg sind, die Anforderungen (in Bezug auf die Sicherheitsaspekte der DSGVO) zu erfüllen. Für Unternehmen, die bisher Probleme hatten, Mittel für Investitionen zu sichern, bietet die DSGVO dagegen eine gute Gelegenheit, Sicherheitsexperten und die Führungsspitze auf einen Nenner zu bringen. Neue Gesetze wie diese zwingen Unternehmen dazu, Mindeststandards einzuhalten, die in Zukunft größere technologische Innovationen fördern.

Datenschutz und IT-Sicherheit stellen nicht nur gesetzliche Auflagen dar, sondern werden auch von Kunden erwartet. Unternehmen werden immer häufiger von ihren Kunden nach dem Umgang mit ihren Daten gefragt. Zwischen Kunden und Unternehmen besteht eine Vertrauensbeziehung, in der sich Kunden darauf verlassen, dass Unternehmen mit ihren Daten vertrauensvoll umgehen. Das Gesetz ist lediglich dazu da, sicherzustellen, dass Unternehmen alles in ihrer Macht stehende tun, um dieses Vertrauen zu rechtfertigen.

Schützen Sie Ihr Unternehmen mit Cisco

Netzwerksicherheit

Was ist Netzwerksicherheit?
Netzwerksicherheit ist eine beliebige Aktivität, welche die Funktionsfähigkeit und Integrität Ihres Netzwerks und Ihrer Daten schützt. Sie umfasst sowohl Hardware- als auch Softwaretechnologien. Eine effektive Netzwerksicherheit verwaltet den Zugriff auf das Netzwerk. Sie geht eine Vielzahl von Bedrohungen an und hält sie davon ab, in Ihr Netzwerk einzudringen oder sich dort zu verbreiten.

Wie funktioniert Netzwerksicherheit?
Netzwerksicherheit kombiniert mehrere Verteidigungsebenen am Netzwerk-Edge und im Netzwerk. Jede Netzwerksicherheitsebene implementiert Richtlinien und Kontrollen. Autorisierte Benutzer erhalten Zugriff auf Netzwerkressourcen, Angreifer werden jedoch davon abgehalten, Exploits und Bedrohungen in Umlauf zu bringen.

Wie profitiere ich von Netzwerksicherheit?

Die Digitalisierung hat unsere Welt verändert sowie die Art wie wir leben, arbeiten, spielen und lernen. Jede Organisation, die von Kunden und Mitarbeitern geforderte Services bereitstellen möchte, muss ihr Netzwerk und urheberrechtlich geschützte Informationen vor Angriffen schützen. Letztendlich dient dies dem Schutz Ihres Rufs.

6 Schritte zum Schutz Ihres Netzwerks

1. Überwachen Sie den Datenverkehr von und zur Firewall und lesen Sie die Berichte sorgfältig. Verlassen Sie sich nicht darauf, dass Sie Warnungen über gefährliche Aktivitäten erhalten. Stellen Sie sicher, dass eine Person in Ihrem Team die Daten lesen kann und bereit ist, die erforderlichen Maßnahmen zu ergreifen.
2. Achten Sie auf neue Bedrohungen, sobald diese entdeckt und online publik gemacht werden. Der Cisco Talos-Blog enthält beispielsweise aktuelle Informationen zu neuen Bedrohungen, Schwachstellen und eine detaillierte wöchentliche Zusammenfassung zu Bedrohungen. Die TrendWatch-Website von Trend Micro verfolgt aktuelle Bedrohungsaktivitäten nach. Außerdem können Sie Warnungen über kürzlich bestätigte Softwareschwachstellen und Exploits vom amerikanischen Computer Emergency Readiness Team (US-CERT, eine Abteilung von Homeland Security) per E-Mail erhalten.
3. Führen Sie regelmäßige Updates Ihrer Firewall und Antivirus-Software durch.
4. Schulen Sie Mitarbeiter regelmäßig, damit diese über jegliche Änderungen an Ihren Richtlinien zur akzeptablen Nutzung informiert sind. Fördern Sie zudem eine Art „Nachbarschaftswache“ als Sicherheitsansatz. Wenn ein Mitarbeiter etwas Verdächtiges bemerkt, etwa wenn er sich nicht sofort bei seinem E-Mail-Konto anmelden kann, sollte er oder sie umgehend den richtigen Ansprechpartner benachrichtigen.
5. Installieren Sie eine Datenschutzlösung. Dieser Gerätetyp kann Ihr Unternehmen vor Datenverlust schützen, falls die Sicherheit Ihres Netzwerks kompromittiert ist.
6. Ziehen Sie zusätzliche Sicherheitslösungen in Betracht, die ebenfalls zum Schutz Ihres Netzwerks beitragen und die Fähigkeiten Ihres Unternehmens erweitern.

Arten von Netzwerksicherheit

Zugriffskontrolle

Nicht jeder Benutzer sollte auf Ihr Netzwerk zugreifen können. Um potenzielle Angreifer fernzuhalten, müssen Sie jeden Benutzer und jedes Gerät kennen. Danach können Sie Ihre Sicherheitsrichtlinien durchsetzen. Sie können nicht konforme Endgeräte blockieren oder Ihnen nur begrenzten Zugriff gewähren. Dieser Prozess wird als Network Access Control (NAC) bezeichnet.

Anwendungssicherheit

Jede Software, die Sie für den Betrieb Ihres Unternehmens ausführen, muss geschützt werden, und zwar unabhängig davon, ob Ihr IT-Personal sie entwickelt oder ob Sie sie kaufen. Leider kann jede Anwendung Sicherheitslücken oder Schwachstellen beinhalten, durch die Angreifer in Ihr Netzwerk eindringen können. Anwendungssicherheit umfasst die Hardware, Software und Prozesse, die Sie zum Schließen dieser Lücken verwenden.

Antivirus- und Malwareschutz-Software

„Malware“, bzw. bösartige Software, umfasst Viren, Würmer, Trojaner, Ransomware und Spyware. Manchmal infiziert Malware ein Netzwerk, bleibt dann aber tage- oder sogar wochenlang inaktiv. Die besten Malwareschutzprogramme scannen nicht nur Malware bei ihrem Eintreten, sondern verfolgen Dateien laufend nach, um Anomalien aufzuspüren, Malware zu entfernen und Schäden zu beheben.

Schutz vor Datenverlust

Organisationen müssen sicherstellen, dass ihre Mitarbeiter keine vertraulichen Informationen außerhalb des Netzwerks versenden. DLP-Technologien (Data-Loss-Prevention; Schutz vor Datenverlust) können Mitarbeiter davon abhalten, kritische Informationen auf unsichere Weise hochzuladen, weiterzuleiten oder sogar auszudrucken.

Verhaltensanalysen

Um ungewöhnliches Netzwerkverhalten erkennen zu können, müssen Sie wissen, was normales Verhalten ist. Tools zur Analyse von Verhaltensanalysen erkennen automatisch Aktivitäten, die von der Norm abweichen. Ihr Sicherheitsteam kann damit Anzeichen für Kompromittierungen besser identifizieren, die ein potenzielles Problem darstellen, und Bedrohungen schnell beseitigen.

E-Mail-Sicherheit

E-Mail-Gateways sind der erste Angriffsvektor für eine Sicherheitsverletzung. Angreifer nutzen persönliche Daten und Social-Engineering-Taktiken, um komplexe Phishing-Kampagnen aufzubauen und damit Empfänger zu täuschen und sie auf Websites mit Malware zu locken. Eine Anwendung für E-Mail-Sicherheit blockiert Angriffe und steuert ausgehende Nachrichten, um den Verlust vertraulicher Daten zu verhindern.

Firewalls

Firewalls bilden eine Barriere zwischen Ihrem vertrauenswürdigen internen Netzwerk und nicht vertrauenswürdigen externen Netzwerken, wie dem Internet. Sie verwenden eine Reihe von

festgelegten Regeln, mit denen Datenverkehr zugelassen oder blockiert werden kann. Eine Firewall basiert entweder auf Hardware, auf Software oder auf einer Kombination aus beidem. Cisco bietet Unified Threat Management-Geräte (UTM) und bedrohungsorientierte Next-Generation-Firewalls.

Intrusion-Prevention-Systeme

Ein Intrusion-Prevention-System (IPS) scannt den Netzwerkverkehr, um Angriffe aktiv zu blockieren. Next-Generation IPS-Appliances (NGIPS) von Cisco korrelieren zu diesem Zweck riesige Volumen an globaler Threat-Intelligence, wodurch nicht nur schädliche Aktivitäten blockiert werden sondern auch der Verlauf von verdächtigen Dateien und Malware im Netzwerk nachverfolgt wird, um die Ausbreitung von Infektionen und Neuinfektionen zu vermeiden.

Sicherheit für Mobilgeräte

Cyber-Kriminelle nehmen zunehmend Mobilgeräte und Apps ins Visier. In den nächsten 3 Jahren werden möglicherweise 90 Prozent der IT-Abteilungen unternehmenseigene Apps auf persönlichen Mobilgeräten unterstützen. Natürlich müssen Sie Kontrolle darüber haben, welche Geräte auf Ihr Netzwerk zugreifen dürfen. Sie werden auch ihre Verbindungsarten konfigurieren müssen, um den Netzwerkverkehr zu schützen.

Netzwerksegmentierung

Bei der softwaredefinierten Segmentierung wird der Netzwerkverkehr unterschiedlichen Klassifizierungen zugeordnet, was die Durchsetzung von Sicherheitsrichtlinien erleichtert. Im Idealfall basieren Klassifizierungen auf der Identität des Endpunkts, und nicht nur auf den IP-Adressen. Sie können Zugriffsrechte basierend auf der Rolle, dem Standort und vielem mehr zuweisen, sodass jeder den passenden Zugriff erhält und verdächtige Geräte eingegrenzt und beseitigt werden.

VPN

Ein virtuelles privates Netzwerk verschlüsselt die Verbindung von einem Endgerät zu einem Netzwerk häufig über das Internet. Normalerweise nutzt ein Remote-Zugriff-VPN IPSec oder Secure Sockets Layer, um die Kommunikation zwischen Gerät und Netzwerk zu authentifizieren.

Websicherheit

Eine Websicherheitslösung überwacht die Internetnutzung Ihrer Mitarbeiter, blockiert webbasierte Bedrohungen und verweigert schädlichen Websites den Zugriff. Sie schützt Ihr Web-Gateway vor Ort oder in der Cloud. „Websicherheit“ bezieht sich auch auf die Schritte, die Sie zum Schutz Ihrer eigenen Website ergreifen.

Wireless-Sicherheit

Wireless-Netzwerke sind nicht so sicher wie kabelgebundene. Ohne strenge Sicherheitsmaßnahmen kann die Installation eines Wireless LAN ausufern und dazu führen, dass überall Ethernet-Ports integriert werden. Damit sich ein Exploit nicht festsetzen kann, benötigen Sie Produkte, die speziell für den Schutz des Wireless-Netzwerks konzipiert wurden.

Threat-Intelligence von Talos

Talos ist die branchenführende Forschungsgruppe von Cisco für Sicherheitsbedrohungen, und alle Cisco Security-Produkte werden durch Talos geschützt. Bei Talos arbeiten über 250 Bedrohungsforscher rund um die Uhr und weltweit mit einer Sammlung von 100 Terabyte Threat-Intelligence.

Wir analysieren täglich ein Drittel des weltweiten E-Mail-Verkehrs und mehr als 2 Prozent der DNS-Anfragen weltweit. Wir beobachten täglich mehr als 1,1 Millionen einzigartigen Malware-Proben durch unsere Advanced Malware Protection (AMP)- und ThreatGRID-Technologie, wodurch wir 19,7 Milliarden Bedrohungen pro Tag in unseren Kundennetzwerken blockieren können.

Sie haben richtig gelesen, 19,7 Milliarden Bedrohungen pro Tag.

Diese umfangreichen Wissens- und Forschungskapazitäten unterstützen die Cybersicherheitslösungen von Cisco, die Transparenz, Automatisierung, Flexibilität und Skalierbarkeit bieten, um Ihre Netzwerkumgebung vor immer ausgeklügelteren Bedrohungen zu schützen.

Cisco Umbrella

Ein Cloud-Security-Service, der integrierten Schutz für Ihren Internetservice bietet

Cisco Umbrella ist ein Cloud-Security-Service, der einen integrierten Schutz vor Angriffen über Ihre Internetverbindung bietet und Ihnen hilft, den Zeit- und Kostenaufwand für die Handhabung von Cyber-Angriffen zu minimieren.

Die Lösung bietet proaktiven Schutz gegen Bedrohungen im Internet, wie Malware, Botnets und Phishing-Angriffe. Sie hilft, Ihr Unternehmen zu schützen, indem sie Datenverkehr bereinigt, bevor er in Ihr internes Netzwerk gelangt. Sie lernt dabei effektiv, von wo Angriffe ausgehen, und blockiert Bedrohungen über alle Ports und Protokolle hinweg. Sie können sich darauf verlassen, dass Sie mit einem sicheren Internetzugriff geschützt sind, der eine erste Verteidigungslinie gegen Malware umfasst.

Cisco Umbrella bietet Transparenz für sämtliche Webanfragen in Ihrem gesamten Netzwerk, für alle Ports, Protokolle oder Apps, um Verbindungen zu schädlichen Domains und IP-Adressen zu erkennen und zu blockieren. Erfahren Sie, warum kleine Unternehmen den Multiplikationseffekt für Sicherheit erreichen, indem sie DNS als Ergänzung vorhandener Sicherheitsmaßnahmen verwenden. Welche Angriffe entgehen Ihnen?

Firewall der nächsten Generation

Eine traditionelle Firewall kann den Verkehr am Ein- oder Austrittspunkt innerhalb des Netzwerks kontrollieren. Mit anderen Worten ist sie die Zugbrücke zwischen Ihrem eigenen Unternehmen und dem " großen unsauberen" Rest des Internets.

Das war perfekt für damals, wo alles noch so einfach war – als Sie noch alles im Blick hatten, was in Ihr Netzwerk kam. Nun, sind Unternehmen zunehmend Gastgeber für eine Vielzahl von unbekannten Geräten und ein tiefes, dunkles Meer mit Cloud-Anwendungen, die von Mitarbeitern heruntergeladen werden.

Der wesentliche Unterschied einer Next-Generation Firewall ist, dass Sie Anwendungskontrollen und Richtlinien festlegen können. Zum Beispiel, wenn einer Ihrer Mitarbeiter eine Dateifreigabe-Software herunterlädt, die möglicherweise unsicher ist, wird Ihnen das automatisch angezeigt, und Sie können sofort reagieren.

Darüber hinaus gewinnen Sie insgesamt weit mehr Transparenz und Kontrolle im Hinblick auf Benutzer, Geräte, Bedrohungen und Schwachstellen in Ihrem Netzwerk. Also, wenn Ihr Vorstand Sie fragt „Sind wir sicher?“, können Sie eine sehr viel umfassendere Antwort geben, als wenn Sie eine traditionelle Firewall haben, die nur den Datenverkehr steuert.

Erfahren Sie mehr über Next-Generation Firewalls oder finden Sie die Next-Generation Firewall, die für Sie am besten geeignet ist.

Advanced Malware Protection

Endpoint-Sicherheit der nächsten Generation

Endpoint-Sicherheit der nächsten Generation ist die Integration von Präventions-, Erkennungs- und Reaktionsfunktionen in einer einzigen Lösung, die das Potenzial von Cloud-basierter Analytik voll ausschöpft. Cisco AMP für Endpunkte ist ein übersichtlicher Connector, der auf Ihren Windows-, Mac-, Linux-, Android- und iOS-Geräten verwendet werden kann.

Cisco AMP für Endpunkte bietet umfassenden Schutz vor besonders komplexen Angriffen. Er verhindert Sicherheitsverletzungen und blockiert Malware beim Eintritt, er erkennt schnell komplexe Bedrohungen, welche die erste Verteidigungslinie durchbrochen haben und in Ihr Netzwerk gelangt sind, dämmt sie ein und beseitigt sie.

Verhindern: Stärken Sie Ihre Abwehr mithilfe von branchenführender, weltweit erfasster Threat-Intelligence und blockieren Sie (nicht) dateibasierte Malware in Echtzeit.

Erkennen: Überwachen Sie alle Dateiaktivitäten fortlaufend und zeichnen Sie sie auf, um getarnte Malware schnell aufzuspüren.

Reagieren: Beschleunigen Sie Untersuchungen und beseitigen Sie Malware automatisch auf PCs, Macs, Linux-Rechnern, Servern und Mobilgeräten (Android und iOS).

Er kann in der Public Cloud verwendet oder als Private Cloud bereitgestellt werden. AMP überwacht und analysiert alle Aktivitäten von Dateien und Prozesse in Ihrem Netzwerk kontinuierlich, um das eine Prozent aller Bedrohungen aufzuspüren, das anderen Lösungen entgeht. AMP verliert nie den Überblick, wohin eine Datei verschoben wird oder was sie tut. Wenn eine Datei, die bei der ersten Untersuchung als unbedenklich eingestuft wurde, jemals schädliches Verhalten zeigen sollte, kann AMP auf den gesamten Verlauf des Bedrohungsverhaltens zurückgreifen, um eine Bedrohung zu erkennen, einzudämmen und zu beseitigen.

Erkennen Sie unbekannte Bedrohungen

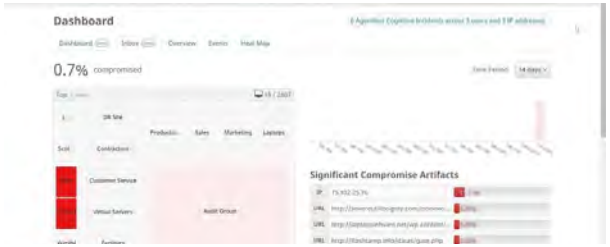
Die integrierte Sandboxing-Technologie von AMP analysiert das Verhalten von verdächtigen Dateien und korreliert es mit anderen Informationsquellen. Die Dateianalyse liefert detaillierte Informationen, damit Sie besser nachvollziehen können, wie der Outbreak eingedämmt und zukünftige Angriffe blockiert werden können.

Wenn eine Datei als schädlich eingestuft wird, reduziert AMP den Zeit- und Ressourcenaufwand für die Untersuchung deutlich. Die Lösung bietet automatisch Einblicke in Ihre drängendsten Fragen, wie:

- Was ist passiert?
- Woher kam die Malware?
- Wo war die Malware?
- Was macht die Malware jetzt?
- Wie kann sie gestoppt werden?

Mit nur wenigen Klicks kann die Datei über die browserbasierte Managementkonsole von AMP blockiert und so verhindert werden, dass sie auf allen Endpunkten ausgeführt wird. Cisco AMP kennt jeden Endpunkt, den die Datei erreicht hat, deshalb kann die Datei für alle Benutzer unter Quarantäne gestellt werden. Mit AMP gleicht die Beseitigung von Malware einem chirurgischen Eingriff. Es entstehen keine weiteren Schäden an den IT-Systemen und Beeinträchtigungen der Geschäftsabläufe werden vermieden.

So stoppen Sie mit Cisco AMP eine Datei und stellen sie unter Quarantäne:



Cisco Meraki

Cloud-Managed Security und SD-WAN

Vollkommen zentralisiertes Cloud-Management für Sicherheit, Netzwerk und Anwendungskontrolle.

Sicherheits-Appliances von Cisco Meraki können in Minutenschnelle und remote per Zero-Touch-Cloud-Provisioning bereitgestellt werden. Die Sicherheitseinstellungen lassen sich mithilfe von Vorlagen über Tausende von Websites hinweg synchronisieren. Die Auto-VPN-Technologie verbindet Zweigstellen sicher und in 3 Klicks über ein intuitives, webbasiertes Dashboard.

Umfassende Sicherheit in einem Paket

Jede Sicherheits-Appliance von Meraki unterstützt mehrere Funktionen, wie eine Stateful-Firewall und eine integrierte Sourcefire Intrusion-Prevention-Engine, um Netzwerke zu schützen. Bedrohungsdefinitionen und Filterlisten werden nahtlos aktualisiert; dadurch wird sichergestellt, dass jeder Standort über Bleeding-Edge-Schutz vor den neuesten Schwachstellen und problematischen Websites verfügt.

Sichern Sie eine Website innerhalb von Minuten

1. Fügen Sie dem Dashboard eine Sicherheits-Appliance von Meraki hinzu.
2. Ermöglichen Sie Intrusion-Prevention.
3. Wählen Sie den gewünschten Schutz vor Bedrohungen.

Mehr erfahren

Aktuelle Informationen und Innovationen finden Sie auf: Cisco Tech Connection für KMU oder entdecken Sie weitere Cisco KMU-Ressourcen und Cisco Security, um Ihr Unternehmen zu schützen.

Vielen Dank für Ihr Interesse.

Sicherheitsgrundlagen für KMU