AVAYA

GANZHEITLICHE SICHERHEIT BIS ZUM NETZWERKRAND – MEHR ALS FIREWALL UND VIRENSCAN

Zu den Auswirkungen eines erfolgreichen Netzwerkangriffs zählen unter anderem:

- Direkte finanzielle Verluste
- Indirekte finanzielle Verluste
- Verlust von Kundenbeziehungen
- Bußgelder und beschränkende Auflagen
- Wertverlust der Marke

Die Herausforderung beginnt bereits im Netzwerk

Unternehmen jeder Form und jeder Größe stellen eine Zielscheibe für Angriffe im und aus dem Internet dar; Gefahren drohen sowohl von internen als auch externen Quellen.

Antiquierte Richtlinien und ein übermäßiges Vertrauen in konventionelle Perimeter-Schutzmaßnahmen sind Gründe dafür, dass Unternehmen nur unzureichend auf Bedrohungen des Digitalzeitalters vorbereitet sind.

Die Herausforderung ist vielschichtig, und genauso differenziert muss auch deren Lösung sein. Es ist jetzt unerlässlich, dass Unternehmen Netzwerklösungen mit integrierten Sicherheitsfunktionen aufbauen.

Top Trends verändern die Netze

Digitalisierung: Immer mehr Geschäftsprozesse werden digitalisiert.

Cloud Computing: Die sichere Bereitstellung relevanter Dienste und Daten an jedem Ort wird immer wichtiger.

Internet of Things: Immer mehr Geräte sind netzwerkfähig und werden mit dem Netz verbunden.

Die **Sicherheitsanforderungen steigen** mit jedem neuen **Gerät, Anwender** und jeder neuen **Anwendung!**

Bedrohung und Auswirkungen mangelhafter IT Sicherheit

Arten der Bedrohung:

- Aktive Bedrohung durch Angreifer
- Passive Bedrohung durch „Verseuchung“
- Belästigung durch Ungewolltes, z. B. SPAM, SPIT, Ransomware

Mögliche Auswirkungen:

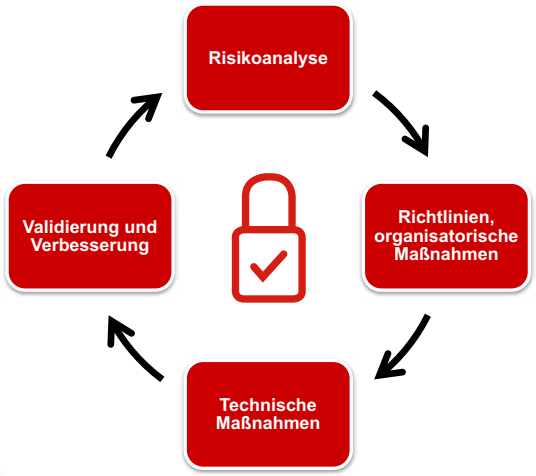
- Persönliche Haftung des Geschäftsführers bei Schäden
- Schlechtere Bonität bei mangelhafter IT Sicherheit
- Imageverlust – Auswirkungen werden nicht öffentlich diskutiert

Bei erfolgreichem Angriff:

- Nicht mehr handlungsfähig durch Virenbefall
- Produktionsausfall
- Ausspioniert, nicht mehr wettbewerbsfähig

Sicherheit als Prozess

Man kauft nicht „ein Stück Sicherheit“ und ist geschützt! Sicherheit ist ein fortlaufender Prozess und umfasst viele Maßnahmen zur Sicherstellung:



IT Sicherheit – wichtiger denn je

Ein Hacker muss kein Experte sein! Hunderte von Werkzeugen stehen zur Verfügung. Programmierkenntnisse sind unnötig. Spezielle Suchmaschinen zum Auffinden von Computern, Druckern usw. erleichtern das Auffinden von potentiellen Angriffszielen.

Hacking / Verwertung von Daten ist eine eigene Industrie geworden! Diese „Branchen” verkaufen / kaufen:

- Daten von Kreditkarten
- Geistiges Eigentum
- Privatsphäre (Bilder usw.)

Bereits einfache Maßnahmen erhöhen die Sicherheit

Beginnen Sie mit der Sensibilisierung und Schulung Ihrer Mitarbeiter. Setzen Sie auf eine klare Kommunikation Ihrer internen Verhaltensregeln zur IT Sicherheit:

Beim Surfen im Internet ist immer Vorsicht geboten

Klicken Sie nicht auf jeden Link, er könnte Sie auf gefährliche Seiten führen.

E-Mail-Sicherheit

Signieren Sie Ihre E-Mails, verschlüsseln Sie sensible Daten, weisen Sie auf potentielle Gefahren hin und seien Sie vorsichtig beim Öffnen von E-Mails und Links.

Soziale Manipulation

Schaffen Sie ein Bewusstsein für den richtigen Umgang mit vertraulichen Informationen, geben Sie diese nur an berechtigte Personen weiter, lassen Sie sich von anderen weder dazu manipulieren oder aushorchen.

Sicherheitsrichtlinien und Unternehmensvorgaben

Definieren und kommunizieren Sie Ihre Sicherheitsrichtlinien, erlauben Sie nur den Gebrauch von geprüften Anwendungen und Software (Apps).

Nur starke Passwörter verwenden

Erlauben Sie nur starke Passwörter. Sie sind mindestens achtstellig und bestehen aus Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen.

Software stets aktualisieren

Nur mit aktualisierter Software schließen Sie mögliche Sicherheitslücken.

Schränken Sie den Zugriff auf Geräte ein

Geben Sie keine Geräte an Dritte weiter, lassen Sie nie Ihre mobilen Geräte unbeaufsichtigt, sperren Sie Ihren PC immer beim Verlassen des Arbeitsplatzes.

Sicherheitsanalyse

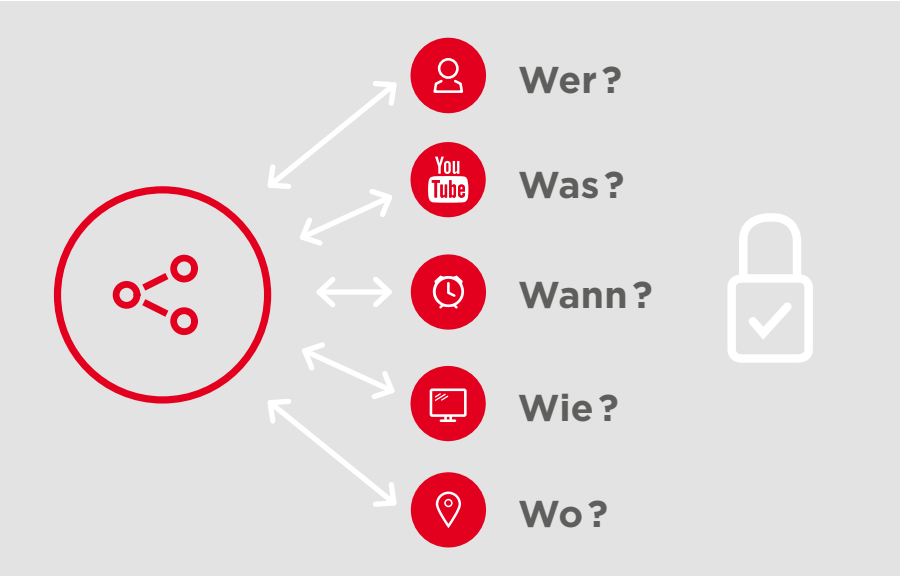
Überprüfen Sie regelmäßig Ihre Sicherheitsmaßnahmen durch interne und externe Sicherheitsanalysen.

Integrierte Sicherheit in Netzwerkkomponenten

Nutzen Sie von Anfang an die in modernen Netzwerk-Lösungen enthaltenen Sicherheitsfunktionen. Wie z. B.: Verschlüsselter Zugang zu den Komponenten und deren Konfigurationen, Authentifizierung, verschlüsselte Datenübertragung im LAN und WLAN, WLAN Applikations-Kontrolle und vieles mehr!

Absicherung von Infrastrukturen

Wer kann im Netzwerk welche Ressourcen wann, wie und wo nutzen?



Einfache, einheitliche und automatisierte kabelgebundene und drahtlose Netzwerke.

Zugang, Steuerung und Kontrolle

Leistungsfähige Network Access Control (NAC) Lösungen schützen Netzwerkbetreiber:

- vor unbefugten Netzwerkzugriffen über das drahtgebundene LAN
- bei der Fernwartung von medizinischen Geräten (z. B. über VPN)
- und ermöglichen den sicheren WLAN-Zugang von Gästen und Partnern auf dem Campus

Kontextbasiertes Richtlinienmanagement für Mitarbeiter und Gäste im gesamten Netzwerk

- Zentralisiertes Richtlinienmanagement
- Durchsetzung von Richtlinien über verteilte Standorte hinweg
- Erweiterbare Durchsetzung der Richtlinien
- Gastzugriffs-Services
- Geräte-Profilierung
- Überwachung und Reporting
- Fehlerbehebung
- Authentifizierung (IEEE 802.1x)

Einsparungen bei Betriebskosten (Produktivität)

Reduzierter Zeitaufwand für Einbindung

- Benutzer – Unternehmen, Auftragnehmer und Gäste
- Kabelgebunden und drahtlos (einschließlich passive Geräte)

Reduzierter Zeitaufwand und weniger Fehler bei Umsetzung der netzwerkweiten Richtlinien

DIE NEUE WELT DER NETZWERK-SICHERHEIT

Schützen Sie sich gegen kostspieligen Datendiebstahl, implementieren Sie Sicherheit auf mehreren Ebenen und umgehen Sie die Schwachpunkte von IP.

Sicherheit überall

Moderne Netzwerktechnologien bieten eine Reihe von Fähigkeiten der nächsten Generation:

Netzwerk-Segmentierung – Erstellen Sie beliebig viele Segmente, die sich nahtlos über das gesamte Netzwerk erstrecken.

–

„Unsichtbare Netzwerke“ - Verbergen Sie Ihre Netzwerke und Daten vor Hackern.

–

Netzwerk-Elastizität durch Automatisierung - Segmente automatisch erweitern und entfernen, wenn sie nicht mehr gebraucht werden.

Höchste Sicherheit, ohne Aufwand!

Früher konnten klare Grenzen am Rand von Filial- oder Campus-Netzwerken eingerichtet und Bereiche bestimmt werden, die sich gegen Zugriffe von außen absichern ließen. Heute muss ein solcher Bereich das Internet of Things (IoT), Besucher, Telearbeiter, persönliche Geräte und mehr unterstützen. Dies erfordert eine höhere Durchlässigkeit und Erweiterbarkeit. Aus unserer Sicht umfassen Lösungen zur Sicherung dieses Gesamtbereichs drei sich ergänzende Fähigkeiten: Segmentierung, „Unsichtbare Netzwerke“ und Netzwerk-Elastizität durch Automatisierung.

Segmentierung: Angriffe verhindern und Hacker isolieren

Die Entkopplung kritischer Applikationen und vertraulicher Daten, die Partitionierung von Geräten und die Errichtung von Barrieren durch Netzwerkrichtlinien sind elementare Netzwerk-Attribute im Zeitalter des IoT.

Netzwerk-Segmentierung leitet Hacker in eine Sackgasse. Wenn ein Segment oder ein Netzwerk angegriffen wird, verhindert die Netzwerk-Segmentierung unberechtigte Zugriffe im restlichen Netzwerk. Mögliche Schäden werden auf ein isoliertes Segment begrenzt. In Zeiten des IoT kommt es auch auf Skalierbarkeit an: Erstellen Sie schnell und einfach eine beliebige Anzahl isolierter Segmente.

„Unsichtbare Netzwerke“: Einhaltung von Compliance und regulatorischen Verpflichtungen

Fabric-basierte Netzwerke stellen ein geschlossenes und unabhängiges Netzwerkkonstrukt mit strikt begrenzter äußerer Erreichbarkeit und geringem sichtbaren Angriffsprofil bereit. Dies erlaubt die Einhaltung von Compliance und regulatorischen Verpflichtungen. Der Aufwand für die Bereitstellung und Wartung eines konvergenten Netzwerks mit Payment Card Industry (PCI)-Unterstützung kann durch den Einsatz Fabric-basierter Netzwerke dramatisch verringert werden.

„Unsichtbare Netzwerke“: Kritische Applikationen und Informationen schützen

Die Gefahrenreduzierung ist für Unternehmen eine absolute Notwendigkeit. Insbesondere in Zeiten, in denen das Risiko einer Cyber-Attacke eher als Regel denn als Ausnahme anzusehen ist. Die meisten veralteten Netzwerke sind offen und einsehbar. Falls ein Hacker eindringt, erlangt er in der Regel Einblick in das gesamte Netzwerk. Moderne Netzwerke sind „unsichtbar“ (Native Stealth) – was man nicht sieht, kann man nicht angreifen. Für Außenstehende bleibt die gesamte Netzwerktopologie unsichtbar – Hacker, die einen Angriff versuchen, sehen lediglich ein „schwarzes Loch“.

Netzwerk-Elastizität durch Automatisierung: Das IoT sichern und verwalten

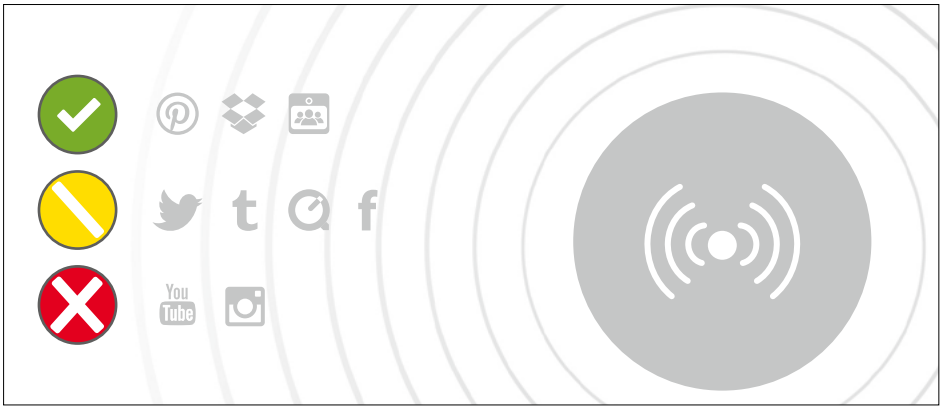
Ein modernes Netzwerk automatisiert die Netzwerkrand-Konnektivität, indem es die Services erweitert oder deaktiviert, abhängig davon, wer oder was die Verbindung herstellt – eine entscheidende Funktionalität im Zeitalter des IoT. Wird ein IP-Telefon angeschlossen, wird das Sprachnetzwerk automatisch und sicher erweitert. Wird eine Überwachungskamera angeschlossen, wird das Überwachungsnetzwerk erweitert. Werden Geräte entfernt, schließt das Netzwerk die Verbindung und verhindert so ein mögliches Eindringen ins Netzwerk durch die Hintertür. Die Agilität der Dienste wird verbessert, die Zugriffskontrolle effektiv erweitert, ungenutzte oder redundante Konfigurationen gelöscht und der Netzwerkrand somit „sauber“ gehalten.

TRANSPARENZ UND KONTROLLE

- Erlauben / Priorisieren
- Drosseln
- Blockieren

Behalten Sie dank intelligenter Applikations-kontrolle die „Lufthoheit“ in Ihrem Wireless LAN!

Aktuelle WLAN-Lösungen bieten granulare Kontrolle von über 1.400 Applikationen.



Transparenz und Kontrolle von Anwendungen:

Die Applikationskontrolle stellt 100 % sicher, das drahtlose Unternehmensanwendungen nicht von Freizeitanwendungen beeinträchtigt werden.

Kontrolle auf Anwendungsebene ist wichtig, da so eine zuverlässige Performance der Anwendung gewährleistet werden kann. Auf diese Weise werden Business-Anwendungen nicht von Freizeitanwendungen behindert. Das gibt IT-Administratoren die Möglichkeit, sehr granular zu kontrollieren, welche speziellen Anwendungen durch welche Benutzergruppen verwendet werden können.

Aktuelle Lösungen erkennen mehr als 1.400 Anwendungen und ermöglichen Unternehmen Anwendungen direkt am Netzwerkrand zu blockieren, zu drosseln oder QoS-Regeln zu vergeben. Sie können zum Beispiel Studenten während der Vorlesung den Zugriff auf Social Media blockieren und eLearning-Anwendungen priorisieren.

So reduzieren Sie die Netzwerkbelastung und sorgen für eine hohe WLAN Qualität für Ihre wichtigsten Anwendungen.

Unser Dienstleistungs-angebot für Sie umfasst:

Beratung / Planung

- Planung von effizienten Netz-werkinfrastrukturen
- WLAN Ausleuchtungen

Installation / Schulungen

- Zertifizierte Techniker
- Onsite & Remote Schulungen

Betrieb

- Ganzheitliche Betreuung Ihrer IT Infrastruktur
- Onsite & Remote Service
- Managed Service

Unser Netzwerk-Portfolio ist breit gefächert:

Switching / LAN

- Netzwerktechnik für EDGE – CORE – Rechenzentrum

Wireless / WLAN

- Indoor / Outdoor / Hotspot Lösungen mit zentralem Management aus Ihrer privaten oder Public Cloud

Security

- Network Access Control / 802.1x Lösungen
- IoT Lösungen
- Firewall

Management / Analyse

- Konfiguration – Überwachung

Konnektivität

- Internetanbindung
- . Standortvernetzung
- . Cloud-Lösungen

Neben dem umfangreichen Netzwerk-Portfolio bietet Ihnen Avaya alles wichtige für eine effiziente Business-Kommunikation:

Seien Sie dem Wettbewerb immer einen Schritt voraus durch den Einsatz unserer vielfältigen **branchenspezifischen Lösungen**, z. B. für das **Gesundheitswesen**.

Steigern Sie die Produktivität durch den Einsatz einer ganzheitlichen Kommunikations-Plattform, die eine schnelle und komfortable **Zusam-menarbeit** Ihrer Mitarbeiter, Kunden und Lieferanten ermöglicht – jederzeit, von überall, auch mobil.

Erhöhen Sie die Zufriedenheit Ihrer Kunden und bieten einen innovativen **Kundendialog** durch den Einsatz flexibler und einfach zu bedienender Kommunikations-Lösungen, die eine schnelle und zuverlässige Erreich-barkeit des richtigen Mitarbeiters sicherstellen.

Profitieren Sie von höherer Effizienz und niedrigeren Gesamtkosten durch die genau für Sie passende Auswahl aus einem breiten Angebot an günstigen, flächendeckend verfügbaren **Sprach- und Daten-anschlüssen**. Betreiben Sie Ihre Kommunikations- Lösungen in einer **Private, Public- oder Hybrid-Cloud**.

Reduzieren Sie die Komplexität und schaffen mit der sicheren, hoch-flexiblen und agilen **Netzwerkinfra-struktur** (LAN/WLAN) die Basis Ihrer Geschäfts-Kommunikation und stellen alle relevanten Daten zuverlässig und jederzeit bereit.

Sichern Sie Ihre Geschäfts-Kommunikation mit den für Sie richtigen Services. Erhalten Sie umfassende Dienstleistungen von Beratung & Design, Implemen-tierung, Betrieb der Lösung, Schulung bis zur Wartung – dazu steht ein eigenes, flächendeckendes Servicenetz bereit.

Setzen Sie Ihr Kapital für Ihr Geschäftswachstum ein. Für die maßgeschneiderte Finanzierung Ihrer Kommunikations-Lösungen bieten wir Ihnen wunschgerechte, umfangreiche Finanzierungsmodelle.

Avaya – Ihr kompetenter Netzwerk-Partner

Reduzieren Sie die Komplexität und schaffen mit der sicheren, hochflexiblen und agilen **Netzwerkinfrastruktur** (LAN/WLAN) die Basis Ihrer Geschäftskommunikation und stellen alle relevanten Daten zuverlässig und jederzeit bereit.

Avaya hilft Ihnen bei der Sicherung Ihre Geschäftskommunikation. Wir bieten Ihnen umfassende Dienstleistungen von der Beratung & Design, Implementierung, Betrieb der Lösung, Schulung bis zur Wartung – dazu steht ein eigenes, flächendeckendes Vertriebs- und Servicenetz bereit.

Fazit

- IT Sicherheit ist spätestens durch die Digitalisierung unverzichtbar geworden
- IT Sicherheit bedarf ständiger Anpassung und Veränderung
- Integrierte Sicherheit ist für jedes Gerät wichtig
- Durch eine Fabric-basierte Lösung können Netzwerkgeräte für den Angreifer unsichtbar werden
- Sicherheit gehört auch an den Netzwerkrand
- Netzwerkzugangskontrolle kann einfach implementiert werden, wie auch BYOD

Interesse?
Gerne besprechen wir mit Ihnen Ihre individuelle Roadmap.

Ganzheitliche Sicherheit bis zum Netzwerkrand – Mehr als Firewall und Virenscan
http://www.avaya.com/de/networking/

Über Avaya

Avaya ist ein führender Anbieter von Lösungen, Services und Endgeräten für die digitale Kommunikation in Unternehmen aller Größen. Unsere offenen, intelligenten und individuellen Lösungen für Contact Center und Unified Communications können flexibel in der als Hybrid-Modell eingesetzt werden. Wir schaffen erfolgreiche Verbindungen und reibungslose Kommunikationserlebnisse für unsere Kunden und deren Endkunden. Unsere professionellen Planungs-, Support- und Management-Service-Teams optimieren unsere Lösungen stetig für einen zuverlässigen und effizienten Einsatz. Avaya Holdings Corp. wird an der New York Stock Exchange unter AVYA gehandelt. Weitere Informationen finden Sie unter **www.avaya.com/de**.

Avaya Deutschland GmbH
Avaya GmbH & Co. KG
Theodor-Heuss-Allee 112
D-60486 Frankfurt/Main
T 0800 GO AVAYA bzw.
T 0800 4 62 82 92
kundensupport@avaya.com
avaya.com/de

Avaya Austria GmbH
Donau-City-Str. 11
A-1220 Wien
T +43 1 87870-0
avaya.at

Avaya Switzerland GmbH
Hertistrasse 31
CH-8304 Wallisellen
T +41 44 878 1414
avaya.ch

Geben Sie uns Ihre Rückmeldung zu diesem Dokument

04/18 Uscha • GE • Änderungen vorbehalten · Gedruckt in Deutschland auf 100% chlorfreiem Papier.