Alcatel-Lucent Enterprise
Cybersicherheit für Unternehmen

Broschüre

Alcatel·Lucent
Enterprise

Überblick

Das Thema Cybersicherheit hat in Unternehmen bereits seit langem höchste Priorität. Durch den stetigen Fortschritt der digitalen Transformation ändern sich auch die Anforderungen an die Cybersicherheit. Digitale Transformation heißt, dass in Netzwerken von Unternehmen und Organisationen vermehrt vernetzte und mobile Geräte eingesetzt werden. Dabei greifen Angestellte verstärkt auf Apps und Daten zu, die außerhalb ihres eigenen Netzwerks liegen.

Und der Wandel vollzieht sich immer schneller: Um mitzuhalten und die Netzwerksicherheit zu gewährleisten, braucht es daher neue Wege. Das vorliegende Dokument bietet Einblicke in die Faktoren, die heutige Anforderungen an die Cybersicherheit von Unternehmen maßgeblich bestimmen. Darüber hinaus werden Strategien und Technologien empfohlen, die Unternehmen einsetzen können, um Daten und Systeme im Zeitalter der digitalen Transformation zu schützen.

Die Cybersicherheits-Lösung von Alcatel-Lucent Enterprise erfüllt die Ansprüche von zunehmend digitalisiert arbeitenden Unternehmen. Mit einem vielschichtigen Konzept für die Cybersicherheit können Unternehmen einen richtlinienbasierten Zugriff auf vernetzte Geräte, sichere Daten und Softwareanwendungen im gesamten Ökosystem des Unternehmens bereitstellen.

Neue Herausforderungen

Die Cybersicherheit wird auf immer neue Art herausgefordert. Mittels künstlicher Intelligenz (KI) und maschinellem Lernen (ML) werden die Angriffe immer raffinierter und sie laufen zunehmend automatisiert ab. Durch neue Techniken des Social Engineering gelingt es Hackern, aus bruchstückhaften Informationen, die quer durch die sozialen Medien auffindbar sind, Profile von Einzelpersonen oder von Datenbeständen zu erstellen, die bei Organisationen und Unternehmen gelistet sind.

Mit der digitalen Transformation in Unternehmen werden auch die Anforderungen an die Cybersicherheit anspruchsvoller: Die Komplexität nimmt zu, es sind immer mehr vernetzte Geräte im Einsatz, es vollzieht sich eine räumliche Entgrenzung – und all das in einem atemberaubenden Tempo.

Mehr Geräte, mehr Komplexität

Unternehmen arbeiten mit neuer Technologie: Cloud, mobile Geräte, Internet der Dinge (IoT), Big Data, Analyse-Tools. Diese modernen Lösungen bringen einen Komplexitätsgrad mit sich, der es erforderlich macht, das Thema Sicherheit ganz neu zu betrachten. Mit der zunehmenden Zahl der vernetzten Geräte nehmen auch die Sicherheitsrisiken und die Möglichkeiten für Datenverletzungen zu.

Bei der ersten Generation vernetzter Geräte gab es beispielsweise nicht einmal eine Passwortabfrage. Da die Geräte mit dem Netzwerk verbunden waren, gelang es Hackern, sich darüber Zugang zum gesamten Netzwerk zu verschaffen. Heutzutage sind Sicherheitsfunktionen wie fest kodierte Passwörter in den Geräten oft vorgeschrieben. Dennoch sind Sicherheitslücken unvermeidlich, und wenn sie auftreten, können sich Hacker immer noch Zugang zum Netzwerk verschaffen.

Räumliche Entgrenzung

Die meisten Organisationen haben lange Zeit klar zwischen Nutzern und Ressourcen inner- und außerhalb des Netzwerks unterschieden. Im Zuge der digitalen Transformation jedoch zeigen sich diese Organisationen nun offener für den Austausch mit einem weiter gefassten Ökosystem, zu dem auch Partner und Dienstleister im Rahmen einer integrierten Kooperationsumgebung gehören. Die Nutzer greifen nicht mehr nur innerhalb der räumlichen Grenzen des Netzwerks auf Ressourcen zu. Sie können sich überall befinden. Informationen können mit Personen in einem anderen Netzwerk ausgetauscht werden. Auch die IT-Ressourcen befinden sich nicht mehr ausschließlich vor Ort im Unternehmen. Sie sind zum Teil räumlich am Standort vorhanden, aber zum Teil auch in eine Cloud ausgelagert oder über APIs vernetzt. Unternehmen benötigen moderne Ansätze zum Schutz der Ressourcen, wenn es keine räumlich klaren Grenzen mehr gibt.

Makro- und Mikrosegmentierung in einer Zero-Trust-Welt

Es gibt zwei Arten der Segmentierung: die Makro- und die Mikrosegmentierung. Bei der Makrosegmentierung wird das physische Netzwerk in verschiedene logische Segmente unterteilt. Alle Unternehmen nutzen die Segmentierung, aber nicht immer aus Sicherheitsgründen. Häufig wird die Makrosegmentierung aus Gründen der Skalierbarkeit, der Verwaltung oder der Organisation eingesetzt. Diese Segmente können ein VLAN, eine Kombination aus VLAN und VRF, ein VPN (Shortest Path Bridging), MPLS oder sogar ein VXLAN oder GRE-Tunnel sein. Der Datenverkehr zwischen Nutzern oder Geräten in verschiedenen Segmenten wird durch eine physische Firewall kontrolliert. Wenn zwei Geräte verschiedenen VLANs zugeordnet sind und kommunizieren können, ohne eine Firewall zu passieren, befinden sie sich im selben Makrosegment. So könnten beispielsweise Kameras und Türschlösser unter die Kontrolle der Gruppe für Zugangssicherheit fallen, während Thermostate unter die Kontrolle der Gruppe für Gebäudewartung fallen könnten.

Die Mikrosegmentierung geht noch einen Schritt weiter. Nicht alle Nutzer sind gleich und nicht alle Nutzer müssen unbedingt auf alle Ressourcen zugreifen können. Ein Profil, das die Nutzer einem Segment zuordnet, enthält auch eine Reihe von Richtlinien, die eine fein abgestufte Kontrolle über die Nutzer-/Geräteberechtigungen ermöglichen. Diese sind für verschiedene Rollen wie die Personal- oder Finanzabteilung unterschiedlich. Dies wird als „rollenbasierter Zugriff" bezeichnet und steht in direktem Zusammenhang mit dem „Prinzip der geringsten Privilegien". Obwohl also Kameras und Türschlösser demselben Segment zugeordnet sind, müssen sie nicht dieselben Ressourcen nutzen. Die Kamera muss mit dem Videorecorder und das Türschloss mit seinem Server kommunizieren. Eine Kamera muss nicht mit einem Türschloss kommunizieren, genauso wenig wie ein Türschloss mit einem anderen Türschloss kommunizieren muss. Diese abgestuften Berechtigungen werden durch Richtlinien umgesetzt, die Teil des Profils sind und nach der Authentifizierung dynamisch auf das Gerät angewendet werden.

Aber brauchen wir wirklich beides? Das Problem bei einem reinen Makrosegmentierungsansatz besteht darin, dass die Firewall zu einem Engpass wird, da alle VLANs an der Firewall abgefangen werden müssen. Dies führt zu Leistungsproblemen. Alternativ können weitere Firewalls auf der Verteilungsebene eingesetzt werden, was jedoch recht kostspielig ist und dennoch keine zufriedenstellende Leistung ermöglicht. Außerdem bedeutet eine größere Anzahl von Firewalls, dass es mehrere Stellen für die Durchsetzung von Richtlinien gibt. Somit gibt es auch mehrere Stellen, an denen die Richtlinien auf dem neuesten Stand gehalten werden müssen.

Eine reine Mikrosegmentierung kann ebenfalls problematisch sein. Wenn die Durchsetzung von Richtlinien ausschließlich über Richtlinien der Netzzugriffskontrolle erfolgt, werden die Richtlinienlisten lang und komplex und können die Kapazitätsgrenzen des Geräts sprengen. Ein Gleichgewicht zwischen diesen beiden Arten der Segmentierung ermöglicht es der Firewall, den Datenverkehr zwischen verschiedenen Segmenten (vertikal) zu kontrollieren, während die Richtlinien der Netzzugriffskontrolle den Datenverkehr innerhalb eines bestimmten Segments (lateral) kontrollieren. Durch die Kombination von Makro- und Mikrosegmentierung kann auf Sicherheitsbedrohungen, die von einem Sicherheitssegment auf ein anderes übergreifen, ebenso reagiert werden wie auf solche, die sich lateral in einem Segment bewegen.

Ein Zero-Trust-Ansatz für die Netzwerksicherheit macht sich das folgende grundlegende Prinzip zu eigen: „Handeln, als ob Angreifer bereits anwesend wären“. Das bedeutet, dass alle Verbindungen authentifiziert werden müssen. Kein Asset und kein Nutzer ist vornherein vertrauenswürdig. Unabhängig davon, ob sie sich auf dem Gelände oder außerhalb des Geländes befinden, werden sie den gleichen Kontrollen unterzogen. Internen Nutzern wird nicht automatisch vertraut. Jeder Zugriff wird authentifiziert.

Betrachten wir ein traditionelles Sicherheitskonzept, bei dem das Netzwerk als eine Art Festung um das Unternehmen herum angesehen wurde. Die Firewall ist diese Festung. Daher gilt alles, was außerhalb der Festung liegt, als nicht vertrauenswürdig und wird überprüft. Alles, was sich innerhalb der Festung befindet, gilt hingegen von vornherein als vertrauenswürdig und zulässig. Die Mikrosegmentierung geht jedoch noch einen Schritt weiter. Dies gilt insbesondere für die softwaredefinierte Mikrosegmentierung. Neben der Firewall und den Sicherheitsvorkehrungen rund um das Gebäude gibt es auch Sicherheitspersonal, das sich ausweisen muss. Diese Vertrauensgrenze ist fließend, räumlich verteilt und flexibel. Sie ist nicht an einen bestimmten Standort, Switch-Port oder an ein bestimmtes VLAN gebunden. Alles hängt von der Identität, dem Gerät, der Situation und der Tageszeit ab. Sie ist softwaredefiniert und wird im laufenden Betrieb angepasst. Das entscheidende Element bei diesem Konzept ist, dass die Komponenten verwaltet werden und in der Lage sein müssen, bei Bedarf auf Bedrohungen oder Änderungen im Arbeitsablauf zu reagieren und Neukonfigurationen vorzunehmen.

Eine Lösung für sich weiterentwickelnde Unternehmen

Alcatel-Lucent Enterprise verfolgt einen ganzheitlichen Ansatz für die Cybersicherheit in Unternehmen. Das mehrschichtige Konzept bietet eine umfassende Sicherheit für vernetzte Geräte und Anwendungen.

Flexible Konnektivität

Unser Ansatz beginnt mit einem flexiblen, autonomen Netzwerk. Das System ermöglicht es, Richtlinien für die Netzwerk- und Cybersicherheit schnell und einfach zu konfigurieren – zum Nutzen der vielen angeschlossenen Benutzer, Geräte und Anwendungen, welche die digitale Transformation vorantreiben.

Früher war die IT vorrangig dafür da, die Hard- und Software im Betrieb am Laufen zu halten. Die IT installierte neue Geräte, setzte sie in Betrieb und verwaltete das Netzwerk, nicht selten in mühevoller Handarbeit. Alcatel-Lucent Enterprise Digital Age Networking bietet ein smartes, automatisiertes Netzwerk, mit dem es ein Leichtes ist, Nutzer und Geräte sicher mit den jeweils benötigten Anwendungen zu verbinden. Digital Age Networking basiert auf der Technologie ALE Intelligent Fabric (iFab) und kombiniert iFab mit dem Industriestandard Shortest Path Bridging (SPB). Nicht nur ist es dadurch einfacher möglich, Netzwerke aufzubauen und zu konfigurieren, sondern die Lösung unterstützt auch schnelles Multipath Routing und Link Aggregation, so dass der Aufbau mehrerer Netzwerkverbindungen parallel möglich ist. Das erhöht den Durchsatz und bietet die notwendige Redundanz.

Beim ALE-Ansatz ist es Aufgabe der IT, Netzwerkdienste, die Architektur, Zugriffsrichtlinien und Container festzulegen. Das Netzwerk selbst baut sich dann automatisch auf. Steht die Architektur des Netzwerks, nimmt das Netzwerk bei jedem Element, das verschoben, geändert oder hinzugefügt wird, automatisch und unbemerkt die notwendigen Anpassungen vor. Wenn zum Beispiel ein Switch ausfällt, umgeht das Netzwerk diesen automatisch.

Ein autonomes Netzwerk bietet Unternehmen den Vorteil der Automatisierung: Das System ist weniger störanfällig, weil kaum noch etwas manuell konfiguriert werden muss, und es ist in der Lage, mit der rasanten Geschwindigkeit mitzuhalten, in der sich die Organisationsstrukturen der Unternehmen weiterentwickeln. Da die IT ihre Zeit dank der Automatisierung nicht

mehr dafür aufwenden muss, Abläufe manuell zu regeln, kann sie wertschöpfend für das Unternehmen tätig werden.

Zugriffskontrolle durch ein intelligentes, automatisiertes Richtlinienkonzept

Mit Digital Age Networking sind Unternehmen in der Lage, Regeln und Richtlinien festzulegen, über die gesteuert wird, welche Zugriffs- und Nutzungsrechte für Anwendungen und Geräte gelten – und sie haben die Nutzer dabei überall im Blick. Sie können zum Beispiel Richtlinien einrichten, die den Zugang zu folgenden Bereichen ermöglichen:

- Spezifische Systeme
- Internet-Dienste
- Andere Partner im Rahmen eines vertraglich vereinbarten Konzepts

Alcatel-Lucent Enterprise bietet außerdem standortbasierte Dienste, etwa zur Orientierung in Gebäuden oder zum Tracking von Equipment und Personen. So können Unternehmen Richtlinien aufsetzen, die den Standort der Nutzer mit einbeziehen.

Die Möglichkeit des Unified Policy Managements (UPAM) bedeutet, dass Nutzungsregeln automatisch durchgesetzt werden, sobald ein Nutzer sich einloggt. So ist sichergestellt, dass Nutzer nur die Zugriffsberechtigung haben, die ihnen zugeteilt wurde. Haben sich Nutzer einmal durch den Login über ein Gerät im Netzwerk legitimiert, ist keine erneute Authentifizierung mehr erforderlich. Solange das Gerät eingeschaltet ist, bleiben die Nutzer eingeloggt und das System achtet darauf, dass die für die betreffenden Nutzer geltende Richtlinienkonzept Anwendung findet.

Auf diese Weise ist gewährleistet, dass alle Nutzer, ob extern oder intern, nur zu zulässigen Bereichen Zugang haben und die Zugriffskontrolle konsequent umgesetzt wird. Das vereinfacht die Abläufe im Unternehmen und stärkt gleichzeitig die Cybersicherheit. Nutzer haben die Möglichkeit, schnell auf benötigte Systeme und Daten zuzugreifen, und werden nicht durch zeitaufwendige Anmeldeprozesse aufgehalten.

Geringeres Sicherheitsrisiko bei Geräten

Unternehmen sind mit zahlreichen IoT-Geräten verbunden. Die Digital Age Networking-Lösung von Alcatel-Lucent Enterprise bietet Organisationen die Möglichkeit, Geräte voneinander zu isolieren. Dazu wird ein virtuelles Netzwerksegment aufgebaut, das verhindert, das ein Gerät zu einem Angriffsziel wird. Containment-Technologie oder auch Containerisierung bedeutet bei Digital Age Networking, dass aus einem einzigen physischen Netzwerk mehrere virtuelle Netzwerke gebildet werden. Die Implementierung ist für die IT-Abteilung mit wenig Aufwand verbunden und die Technologie kann über ein einziges Managementsystem verwaltet werden. Diese Lösung erkennt automatisch jedes einzelne Gerät im Netzwerk. Wird ein Gerät mit dem Netzwerk verbunden, versucht das Alcatel-Lucent OmniVista® Network Management System, das entweder vor Ort oder in der Cloud betrieben wird, dieses Gerät zu identifizieren. Ist das Gerät nicht in der Datenbank des Systems verzeichnet, wird eine cloudbasierte Datenbank, die über 29 Millionen Geräte enthält, abgefragt.

Ist das Gerät erkannt, wird es vom System einer Kategorie zugeordnet, etwa als Sicherheitskamera. Steht das Gerät auf der Freigabeliste für Lieferanten von Sicherheitskameras, wird es mit dem Netzwerk verbunden. Falls nicht, wird die Verbindung verweigert. Die Lösung wird dann in einem virtuellen Container für das Gerät installiert, der es vom Rest des Netzwerks isoliert. Wenn nun ein Angreifer in ein vernetztes Gerät eindringt, kann er das betreffende Gerät nicht für den Zugriff auf das restliche Netzwerk missbrauchen.

Künstliche Intelligenz für eine vertrauenswürdige Umgebung

Sind Geräte mit dem Netzwerk verbunden, müssen sie kontinuierlich überwacht werden, damit Gefahren rechtzeitig erkannt werden und das Vertrauen in die Arbeitsumgebung erhalten bleibt. Über die Funktionalität, die Alcatel-Lucent Enterprise im Bereich der Analyse und Sichtbarkeit bietet, haben Netzwerkadministratoren für jedes einzelne Gerät stets im Blick, was im Netzwerk passiert. Die Analyse-Werkzeuge erkennen, welche Muster ein normales, erwartetes Verhalten im Netzwerk darstellen, aber auch Abweichungen. Das Verhalten von Anwendungen am Rand des Netzwerks kann überwacht werden, um dann zu entscheiden, ob eine Verbindung zu dieser Anwendung zugelassen wird. Auch ungewöhnliches Verhalten von Anwendungen, die bereits im Netzwerk sind, fällt auf, zum Beispiel, wenn eine Kamera mehr Daten generiert als erwartet.

Zeigt ein Gerät ein ungewöhnliches Verhalten, ist das über die Analyse-Werkzeuge zu sehen. Dann kann der für das Netzwerk zuständige Sicherheitsmanager eingreifen. Bisher erfolgt die Untersuchung eines Vorfalls noch manuell, das Unternehmen arbeitet jedoch daran, die Reaktion mittels KI und ML zu automatisieren.

Schutz des Netzwerks

Zwar wissen Unternehmen heutzutage, dass IoT-Geräte im Netzwerk durch Sicherheitsvorkehrungen geschützt werden müssen, doch werden Geräte wie etwa Switches und Zugangspunkte, die die Grundlage des Netzwerks bilden, möglicherweise nicht berücksichtigt. Alcatel-Lucent Enterprise senkt mit unterschiedlichen Technologien das Gefahrenpotenzial dieser Geräte. Lösungen:

- Absicherung der Betriebssystem-Software für einen sicheren, diversifizierten Code.
- Prüfung und Validierung der Betriebssystem-Software durch Dritte, damit sichergestellt ist, dass es keine angreifbaren Einstiegspunkte oder Hintertüren gibt.
- Immer wenn ein Switch bootet, wird der Speicher unterschiedlich kompiliert und bereitgestellt. Zwar funktionieren alle Switches gleich, die interne Speicherkonfiguration unterscheidet sich jedoch von Gerät zu Gerät. Gelänge es Angreifern, einen Switch von Alcatel-Lucent Enterprise zu hacken, hätte der Angriff bei keinem zweiten Switch auf diese Weise Erfolg.
- Schutz durch integrierten Denial of Service (DoS). Die CPU erkennt ein ungewöhnliches Aufkommen beim Datenverkehr im Netzwerk und schaltet sich ggf. automatisch ab.
- Mehrere Sicherheitszertifizierungen nach verschiedenen Standards, u. a. JDIC und FIPS.
- Kontinuierliche Software-Upgrades

Sichere Verbindungen für ein- und ausgehenden Datenverkehr

Für eingehenden Datenverkehr bieten unsere VPN-Funktionalitäten eine verschlüsselte Verbindung zum lokalen Netzwerk. Ende-zu-Ende-Verkehr wird über MACsec (auch als IEEE 802.1AE bekannt) verschlüsselt, damit die Daten geschützt sind, wenn sie das Netzwerk durchqueren. Durch die Möglichkeit, Dienste ohne Reboot erneut zu laden, etwa TLS und HTTPS, läuft das Netzwerk unterbrechungsfrei.

Berichte

Über das Reporting, das Alcatel-Lucent Enterprise bietet, haben verschiedene Stellen im Unternehmen Zugriff auf Daten, die Aufschluss über den Status, die Stabilität und die Leistung des Netzwerks geben und anzeigen, wie die Anwendungen laufen. Auch die Benutzerzufriedenheit kann abgefragt werden. Die IT sieht jederzeit die Daten zur Netzwerkleistung und zu den Netzwerkprozessen.

Geschäftsbereiche können über das Reporting feststellen, ob ihre Geräte, zum Beispiel Sensoren oder Telemetriesysteme, die Daten störungsfrei an Server und Tablets übertragen. Die IT-Abteilung kann prüfen, ob das Netzwerk die Dienste bereitstellt, die es Mitarbeitern ermöglichen, sich ohne unnötige Zeitverluste ganz ihren Aufgaben zu widmen, und ob das Netzwerk als Ressource optimal ausgeschöpft wird.

Cybersicherheit in verschiedenen Branchen

Bildungswesen

Durch die Einführung von Smart-Campus-Strategien in Bildungseinrichtungen wird es mehr vernetzte und mobile Geräte in deren Netzwerken geben, und die Geräte im Internet der Dinge (IoT) werden immer häufiger auf Anwendungen und Daten von außerhalb des Netzwerkperimeters zugreifen.

Die Vernetzung und Innovation großer Campus-Infrastrukturen macht diese zu einem direkten Ziel für Cyberbedrohungen. Das von Alcatel-Lucent Enterprise angebotene Digital Age Networking für den Smart Campus sorgt für die Sicherheit von IT-Ressourcen und Daten im heutigen Zeitalter der digitalen Transformation. Mit dieser Lösung können Einrichtungen den Benutzerzugriff gezielt verwalten. Darüber hinaus sind sie in der Lage, die durch das Internet der Dinge, Mobil- und Netzwerkgeräte verursachten Sicherheitsrisiken einzudämmen und zu verhindern, dass die unvermeidliche Sicherheitsverletzung zu einem Angriffspunkt wird. Gleichzeitig können sie ihren Studenten und Mitarbeitern problemlos alle Dienste und Anwendungen zur Verfügung stellen, die von ihnen benötigt werden.

Transport und Verkehr

Die aus den technologischen Innovationen resultierenden Fortschritte bei den Verkehrssystemen erfordern eine Umgestaltung des jetzigen Fundaments der Systeme. Die Integration der Geräte und Systeme, die das Funktionieren eines Transportökosystems ermöglichen, erfordert schnelle, zuverlässige und sichere Verbindungen. Verkehrsdatennetze müssen IoT-fähig sein, um Sensoren, Kameras, Beschilderungen und Verkehrsleitsysteme nahtlos miteinander verbinden zu können. Die Netzwerksicherheit ist auch für den Schutz der Daten und der Integrität des Netzes von entscheidender Bedeutung.

Alcatel-Lucent Enterprise verwendet einen sicheren, diversifizierten Code, um die Netzwerkintegrität zu verbessern und zusätzlichen Schutz vor Cyberangriffen auf das Netz zu bieten. Der sichere, diversifizierte Code schützt das Netzwerk vor Sicherheitsrisiken, der Ausnutzung von Lücken im Code, Malware und potenziellen Backdoors, die geschäftskritische Vorgänge gefährden könnten. Alcatel-Lucent Enterprise bietet zudem eine Fingerprinting-Technologie für das Internet der Dinge (IoT), um jedes Gerät, einschließlich Fahrzeuge, Sensoren und Kameras, anhand von Fingerabdrücken zu identifizieren und sicherzustellen, dass sie keine Sicherheitsbedrohung für das Netzwerk darstellen. Die umfassende Sicherheitsstrategie hat die höchsten Zertifizierungsstufen von Regierungsbehörden erhalten, darunter Common Criteria (EAL2 und NDcPP), JITC, FIPS 140-2 und NIST.

Gesundheitswesen

Das Gesundheitswesen ist schon seit langem, und auch weiterhin, eine Branche, die besonders im Visier der Hacker steht. Und dieses Problem scheint weiter um sich zugreifen. 2018 verzeichnete das Gesundheitswesen 503 Cyberangriffe, die 15 Millionen Patientenakten betrafen, drei Mal so viel wie 2017, laut dem Protenus Breach Barometer.[1]

Diese Cyberangriffe gibt es, weil Gesundheitsdaten extrem wertvoll sind. Patientenakten enthalten eine Menge persönlicher Daten: Name, aktuelle und frühere Adressen, berufliche Laufbahn, Namen und Alter der Angehörigen sowie Finanzdaten, etwa Kreditkartennummern und Kontodaten.[2]

Digital Age Networking setzt als Cybersecurity-Konzept gleich an mehreren Punkten an. Der Zugang zu vernetzten medizinischen Geräten, Patientendaten und Software-Anwendungen im Ökosystem des Gesundheitswesens erfolgt sicher und nach exakt festgelegten Regeln: DAN bedeutet Vertraulichkeit.

Öffentlicher Sektor

Die stärkere Rolle der Digitalisierung sowohl auf zentraler Regierungs- als auch auf städtischer Ebene hat die Grenze zum Schutz digitaler Ressourcen verwischt, die den Transport, die Wartung der Infrastruktur und die Umweltüberwachung gewährleisten. Die staatlichen Cybersicherheitsrichtlinien für das Management von Datensicherheit, Sicherheitsrisiken und vertrauenswürdigen Quellen müssen überarbeitet werden.

Der ALE-Ansatz zur Cybersicherheit bietet einen serviceorientierten Ende-zu- Ende-Sicherheitsansatz, der alle Ebenen des Service schützt, vom Netzwerk bis zur Software. Auf der Geräteseite können Organisationen des öffentlichen Sektors die Containerisierung nutzen, um ein virtuelles Netzwerksegment zu schaffen, das verhindert, dass Geräte zu Angriffspunkten werden.

Hotel- und Gastgewerbe

Der vermehrte Einsatz des Internets der Dinge (IoT) im Hotel- und Gastgewerbe bringt eine Explosion von Bedrohungen für die Cybersicherheit mit sich, da die Verbreitung von Sensoren und angeschlossenen Geräten die Angriffsfläche für das Netzwerk erheblich vergrößert. Das Internet der Dinge ist besonders anfällig, da viele IoT-Geräte ohne Rücksicht auf die Sicherheit hergestellt oder von Unternehmen entwickelt werden, die die aktuellen Sicherheitsanforderungen nicht kennen. Folglich sind IoT-Systeme immer häufiger das schwache Glied in der Netzwerksicherheit von Unternehmen des Hotel- und Gastgewerbes.

Für den Schutz von IoT-Datenverkehr und -Geräten wird ein strategischer Ansatz benötigt, in dessen Rahmen die Vorteile mehrerer Sicherheitsvorkehrungen kombiniert werden. Um Hotels, Casinos, Resorts und andere Unternehmen des Hotel- und Gastgewerbes dabei zu unterstützen, die Vorteile des IoT-Einsatzes zu nutzen und die Risiken zu minimieren, bietet ALE eine mehrstufige Sicherheitsstrategie, die Schutz auf jeder Ebene der Infrastruktur bietet – vom einzelnen Benutzer und Gerät bis hin zur Netzwerkebene. Alcatel-Lucent Enterprise hat darüber hinaus eine IoT-Risikoeindämmungsstrategie ausgearbeitet, um das Onboarding von Geräten zu vereinfachen und abzusichern. Im Zuge dieser Strategie werden die richtigen Netzwerkressourcen für den ordnungsgemäßen und effizienten Betrieb des Systems bereitgestellt – und das alles in einer sicheren Umgebung, damit Unternehmen des Hotel- und Gastgewerbe vor Cyberangriffen geschützt sind.

1 https://healthitsecurity.com/news/the-10-biggesthealthcare-data-breaches-of-2019-so-far

2 https://www.forbes.com/sites/mariyayao/2017/04/14/your-electronic-medical-records-can-be-worth-1000-tohackers/#2bb1f96b50cf

Zusammenfassung

Immer mehr vernetzte Geräte, räumliche Entgrenzung, Veränderungen, die sich immer schneller vollziehen: Im Zuge der digitalen Transformation haben sich die Anforderungen an die Cybersicherheit in Unternehmen fundamental gewandelt. Digital Age Networking von Alcatel-Lucent Enterprise sorgt für die Sicherheit von IT-Ressourcen und Daten im heutigen Zeitalter der digitalen Transformation. Mit dieser Lösung können Sie den Benutzerzugriff gezielt verwalten und Sicherheitsrisiken eindämmen, die durch IoT-, Mobil- und Netzwerkgeräte entstehen. So können Sie verhindern, dass die unvermeidliche Sicherheitsverletzung zu einem Angriffspunkt wird, und ein vertrauenswürdiges Unternehmensökosystem bereitstellen.

DID21071901EN (Juli 2024)