INFRASTRUKTUREN FÜR TRANSPORT & VERKEHR SICHERN

EIN BEWEGLICHES ZIEL: WARUM DIE SICHERUNG VON IT-SYSTEMEN IM VERKEHRSWESEN IMMER SCHWIERIGER WIRD

EINLEITUNG:
CYBERSICHERHEIT IM VERKEHRSWESEN

Seit ihrer Einführung vor Jahrzehnten waren die Computersysteme, auf die der Verkehr in Europa wie der ganzen Welt angewiesen ist, Einzelsysteme, die nicht mit anderen Systemen oder dem Internet verbunden sind. Flugverkehrskontrolle, Bahnsignal- und -leitsysteme, industrielle Steuersysteme für die Schifffahrt – jedes war physisch von allen anderen Netzen getrennt, eine Praxis, die als „Air Gap" bezeichnet wird. Aufgrund der kritischen Bedeutung von Transport und Verkehr für das Gemeinwesen mussten sich die Entwickler auf die Systemverfügbarkeit und Interoperabilität konzentrieren, allerdings nicht unbedingt auf die Cybersicherheit. Daher wurde diese Praxis der Air Gaps zum wichtigsten Sicherheitsmerkmal, das kritische Systeme vor dem Eindringen oder Cyberangriffen von außen schützte.

Die Intransparenz dieser Systeme, die in vielen Fällen auf eigenen, herstellerspezifischen Komponenten und Kommunikationsprotokollen basieren, bestärkte die Auffassung, integrierte Sicherheitsfunktionen seien nicht wirklich erforderlich. In den letzten zehn Jahren jedoch führten Geschäftsziele, wie die Notwendigkeit zur Senkung von Kosten, Verbesserung der betrieblichen Effizienz, Erfüllung regulatorischer Auflagen und Bereitstellung einer ganzheitlichen Übersicht des Anlagenbetriebs zu einer Veränderung der Sicherheitslage. Vor allem seit das Konzept des Internets der Dinge (IoT) – einschließlich der intelligenten Verkehrssysteme (ITS) – in die Verkehrsnetze integriert wurde, ist die Strategie der Air Gaps zunehmend unhaltbar geworden.

In vielen Bereichen der internationalen Verkehrs-IT hat zudem Integration von kosteneffizienten und stärker vernetzten IT-Technologien sowie Commercial-of-the-Shelf-(COTS)-Produkten in die Betriebsumgebung stattgefunden. IT-Systeme des Transport- und Verkehrswesens sind heute über das Internet stärker mit geschäftlichen Systemen in Unternehmensnetzwerken und sogar mit der Außenwelt vernetzt. Diese Veränderungen führen zu einer Reihe von Sicherheitsschwachstellen, die im allgemeinen IT-Bereich bereits bekannt sind, für den Transport und Verkehr jedoch neu sind. Entscheidungsträger für IT müssen künftig diese Bedrohungen der Cybersicherheit besser verstehen und ihnen effizient begegnen.

ÜBERSICHT ÜBER DEN VERKEHRSSEKTOR

> Ein großes, komplexes, vernetztes System wie der NAS ist naturgemäß zahlreichen Sicherheitsrisiken ausgesetzt. Obwohl die Luftverkehrsbehörde FAA viel getan hat, um diesen Risiken zu begegnen, bestehen nach wie vor Schwachstellen, die für die FAA bei der Erfüllung ihrer Aufgabe, Sicherheit und Effizienz des Flugverkehrs zu gewährleisten, herausfordern."

Quelle: US Government Accountability Office

Verkehrssysteme und Rahmenbedingungen für Cybersicherheit

Um das Ausmaß der Herausforderungen für die Cybersicherheits zu verstehen, denen sich der internationale Verkehrssektor gegenübersieht, lohnt es sich, einige der in Betracht kommenden Kernsysteme und Ansätze zur Sicherung der IT zu untersuchen. Dabei sind auch die IoT-Trends zu berücksichtigen, die die Art und Weise, wie Personen und Waren im 21. Jahrhundert befördert werden, verändern. Aus Platzgründen konzentrieren wir uns hier auf nordamerikanische und europäische Verkehrssysteme und regulatorische Rahmenbedingungen. Man sollte jedoch daran denken, dass die hier beschriebenen Probleme der Cybersicherheit weltweit für die Verkehrsinfrastruktur gelten.

National Airspace System (NAS)

Das NAS (Nationales Luftraumsystem) umfasst die Infrastruktur der USA für den Flugverkehr, einschließlich Flughäfen, Flugsicherungsanlagen und -systemen, Radaranlagen und Kommunikationsvermittlung. Im Durchschnitt nutzen täglich rund 50.000 kommerzielle und militärische Flüge die Dienste des NAS. Das jetzige NAS setzt seit langem auf eine Kombination mehrerer Netzwerke und zahlreiche Punkt-zu-Punkt-Verbindungen – dies sind Kommunikationssysteme, die physisch vom Internet isoliert sind. Schwachstellen bei der Cybersicherheit im NAS sind jedoch Computer, die die Schnittstellen des Flugverkehrssystems kontrollieren und schützen, Benutzer identifizieren und authentifizieren sowie Benutzerzugriff gewähren.

Bahnsignalsysteme

Aufgrund ihrer historischen Entwicklung behielten private Eisenbahnunternehmen eine proprietäre Signalinfrastruktur bei und gab es in der diesem Verkehrsbereich wenig Standardisierung. Wie bei der Luftfahrt werden jedoch auch Steuerungssysteme der Eisenbahnen stärker mit dem öffentlichen Internet integriert. In zunehmendem Maße übernehmen Signalisierungs- und Steuersysteme Aspekte industrieller Steuersysteme (ICS), darunter Elemente von Überwachungs- und Datenerfassungssystemen (SCADA). Mit zunehmender Standardisierung von Kommunikationssystemen und eingesetzten Geräten werden diese Systeme anfälliger für Cyberangriffe und Malware.

ÜBERSICHT ÜBER DEN VERKEHRSSEKTOR (FORTSETZUNG)

> Die Gewährleistung der Cybersicherheit hat sich auf nationaler und internationaler Ebene zu einer zentralen Herausforderung für Staat, Wirtschaft und Gesellschaft entwickelt. Die Cybersicherheits-Strategie soll die Rahmenbedingungen in diesem Bereich verbessern."
>
> Quelle: Bundesamt für Sicherheit in der Informationstechnik

ISAC für europäische Eisenbahnen

Ende 2017 trafen sich hochrangige Vertreter der europäischen Eisenbahnbranche und der Informationssicherheit in Brüssel zur Konferenz CyberSecurity4Rail, um die Bildung eines europaweiten Information Sharing and Analysis Centre (ISAC) zu erörtern, das als übergreifender Ansatz für die Cybersicherheit für diesen Verkehrsbereich gedacht ist. Die Tagung folgte auf die Verabschiedung der EU-Richtlinie zur Netzwerk- und Informationssicherheit (NIS-Richtlinie1), die im Juli 2016 vom Europäischen Parlament beschlossen und zeigte den künftigen Weg für Cybersicherheit im Bereich der Bahn-IT in ganz Europa auf. Im Rahmen dieses Prozesses berufen die EU-Mitgliedstaaten nationale CSIRTs (Computer Security Incident Response Teams) oder CERTs (Computer Emergency Response Teams) und richten Kommunikationskanäle ein, um sich gegenseitig über Bedrohungen und Vorfälle zu informieren und Best Practices für die Cybersicherheit im Bahnbereich zu fördern.

KRITIS in Deutschland

Die NIS-Richtlinie der EU bildet den Rahmen für die Cybersicherheit im Verkehrsbereich in ganz Europa, doch die einzelnen EU-Mitgliedstaaten haben weiterhin die Verantwortung für ihre eigenen Transport- und Infrastrukturnetze aus. Das deutsche KRITIS ist hierfür ein Beispiel. KRITIS umfasst die Verkehrsinfrastruktur in Deutschland sowie die Kritische Infrastruktur der Bereiche Energie, IT, Gesundheitswesen, Finanzdienstleistungen, Wasser und Ernährung und legt klare Bestimmungen zur Cybersicherheit auf der Grundlage eines Ansatzes der „Risikokultur" fest. KRITIS fordert von den Beteiligten eine Selbstverpflichtung hinsichtlich der Verhütung und des Managements von Zwischenfällen, offene Kommunikation zwischen Staat, Unternehmen, Bürgern und der Öffentlichkeit im alggemeinen und Zusammenarbeit aller Beteiligten bei der Verhinderung und Bewältigung von Zwischenfällen.

ÜBERSICHT ÜBER DEN VERKEHRSSEKTOR (FORTSETZUNG)

> “Die stärkere Nutzung von IP-Netzwerken zur Verbindung von Systemen und Diensten im NextGen-Zeitalter wird negative Auswirkungen auf die bisherigen Lösungen für Ausfallsicherheit, Redundanz und Abschottung haben. Durch die stärkere Vernetzung von Systemen werden auch die Cyberrisiken für das NAS erhöht.”
>
> Quelle: US-Luftverkehrsbehörde FAA

Die nächste Generation von Verkehrssystemen

Die Systeme des Luft- wie des Schienenverkehrs haben tiefgreifende Veränderungen durchlaufen und werden in den nächsten Jahren durch die Möglichkeiten des IoT völlig umgestaltet. Die tiefgreifendsten Veränderungen des Verkehrsbereichs in den kommenden Jahren wird jedoch im Automobilsektor erfolgen, sowohl durch intelligente Fahrzeuge als auch durch automatisierte Autobahn- und Straßennetze.

IoT Intelligente Straße und Infrastruktur

In den Medien finden vor allem autonome Fahrzeuge Beachtung, aber die weitreichendsten Veränderungen werden sich durch intelligente Straßen ergeben. Kürzlich durchgeführte europäische Studien zu intelligenten Verkehrssystemen (IVS) haben gezeigt, dass Straßen, die mit Sensoren, Radar, Profilometern, Kameras und drahtlosen, in das öffentliche Internet integrierten Netzwerken ausgestattet sind, ein großes Potenzial für einen reibungsloseren Verkehrsfluss bieten, die Verkehrssicherheit steigern und die Möglichkeiten von intelligenten Fahrzeugen besser nutzen können. Automobilhersteller entwickeln Pläne zur Ausstattung von Fahrzeugen mit 5G-Vernetzung, was praktisch unbegrenzte Möglichkeiten für eine verbesserte Navigation, Automatisierung und Onboard-Dienste bieten wird. Aber gleichzeitig dem Ausbau dieser intelligenten Infrastruktur wird es immer wichtiger, sichere Kommunikation für V2V (Fahrzeug zu Fahrzeug), V2P (Fahrzeug zu Fußgänger), V2I (Fahrzeug zu Infrastruktur) und V2C (Fahrzeug zu Cloud) zu ermöglichen.

NAS NextGen

Die US-Luftverkehrsbehörde FAA aktualisiert ihre wichtigsten Flugsicherungssysteme auf der Grundlage von Internetprotokollen. Teil dieses Upgrades ist die Umstellung auf ein satellitengestütztes Navigationssystem, das genauer ist als bodengestützte Navigationssysteme. Künftig werden Flugzeuge mit einer satellitengestützten GPS-Navigationstechnologie ausgestattet sein, die ständig ihren Weg an die Flugsicherung übermittelt. Es wird erwartet, dass der Anteil des NAS-Systems, das IP-Netzwerke nutzt, bis 2020 auf 50 bis 60 Prozent ansteigen wird. Diese Verlagerung hin zur IoT-Architektur wird tiefgreifende Auswirkungen auf die Cybersicherheit haben, so dass Systemadministratoren Sicherheitsstrategien entwickeln müssen, die fortlaufende Sicherheitsanalysen und Überwachung sowie Verhinderung von Eindringversuchen umfassen.

HERAUSFORDERUNGEN BEI BETRIEB UND SICHERHEIT DES VERKEHRSWESENS

Die vielen, unterschiedlichen und zunehmenden Schwachstellen in der Transport-IT-Infrastruktur stellen eine ganze Reihe von Risikofaktoren dar, die potenziell weitaus schädlicher sein können als die typischen Datenschutzverletzungen im Einzelhandel, bei Banken oder anderen verbraucherorientierten Unternehmen. Negative Berichterstattung, Imageschäden und behördliche Bußgelder können zwar für betroffene Unternehmen teuer werden, betreffen aber in der Regel nicht die Sicherheit von Personen. Bei Verkehrssystemen ist dies anders. Hier ist Folgendes zu bedenken:

1. Steigende Betriebskosten

Die Umsetzung von Sicherheitskontrollen zur Minderung der mit diesen Sicherheitslücken verbundenen Risiken kann, sofern nicht sorgfältig geplant, äußerst kostenintensiv sein. Die IT erfordert ein hohes Maß an Kompetenz von qualifizierten Mitarbeitern. Hinzu kommt, dass solche Mitarbeiter infolge der alternden Belegschaft bereits stark nachgefragt sind. Unternehmen stellen bei der Umsetzung intern entwickelter Lösungen häufig fest, dass diese nicht umfassend genug sind, sich nur schwer implementieren lassen und viel Zeit für Unterhaltung in Anspruch nehmen.

2. Zunehmende Gefahr von Betriebsunterbrechungen

Mögliche Folgen eines unbefugten Zugriffes auf Verkehrssysteme und einer möglichen Manipulation physischer Geräte sind unter anderem Schäden an Anlagen, negative Folgen für den Betrieb, Produktverluste, Umweltbelastungen und sogar der Verlust von Menschenleben. Das Verständnis der potenziellen Risiken kann Unternehmen helfen, einen nachhaltigen Plan zur Beseitigung der Schwachstellen mit den größten Auswirkungen auf den Betrieb zu entwickeln. Experten sind sich einig, dass der Einsatz von allgemein üblichen Computern in Steuerungssystemen das größte Risiko für Sicherheitsverletzungen darstellen, da sie in der Regel auf gängigen Betriebssystemen basieren. Die Verbindung zu internen Netzwerken (Geschäftssysteme in der IT-Infrastruktur) sind das zweitgrößte Risiko. Beide Risiken können ausgenutzt werden, indem Angreifer an privilegierte Anmeldedaten gelangen, um sich Zugang zu diesen wichtigen Ressourcen zu verschaffen.

3. Compliance mit Vorschriften

Unternehmen sowie Behörden haben erkannt, dass der Schutz Kritischer Infrastrukturen direkt von der Sicherheit der Steuerungssysteme abhängt, die die verschiedenen Prozesse in den Bereichen Luft- und Schienenverkehr sowie zunehmend auch von intelligenten Straßen steuern. In der Folge unterliegen Branchen mit kritischer Infrastruktur der behördlichen Aufsicht oder müssen in ihren OT-Umgebungen spezielle Cyber-Sicherheitsstandards erfüllen. Es besteht ein Bedarf an Tools und Workflows, die Unternehmen beim Nachweis ihrer Compliance mit diesen Standards und Vorschriften unterstützen.

> **“Cyberbedrohungen für Informationssysteme auf nationaler Ebene, wie die, auf die sich die FAA für ihre ATC-Systeme stützt, entwickeln sich ständig weiter. Diese Bedrohungen können absichtlich oder unbeabsichtigt sein und aus einer Vielzahl von Quellen stammen, wie Kriminellen, fremden Staaten, Terroristen und anderen gegnerischen Gruppen.”**
>
> Quelle: U.S. Government Accountability Office

SICHERHEITSLÜCKEN IN VERKEHRSSTEUERUNGSSYSTEMEN

Übermäßiger Einsatz von Administratorkonten

Die Zahl der Benutzer und Anwendungen, die (im Unternehmen und über Remote-Zugang) Betriebsdaten aus der IT im Verkehrswesen abrufen und extrahieren, ist stark gestiegen. Dies dürfte zum Teil auf die Notwendigkeit zurückzuführen sein, Entscheidungsträgern mehr Einsicht in und verwertbare Information über ihren Betrieb zu bieten und den Remote-Zugriff für Dritte und mobile Mitarbeiter zu ermöglichen. Die für den Zugriff auf industrielle Netzwerke und kritische Systeme erforderlichen privilegierten Accounts und Administratorkonten sind in der Regel zahlreich vorhanden und werden in vielen Fällen nicht verwaltet. Support- und Wartungspersonal sowie Bedienpersonal und Steuerungstechniker, Remote-Anbieter, Unternehmensanwendungen und automatisierte Batch-Anwendungen nutzen alle solche privilegierten Accounts. Diese große Anzahl von Konten erschwert ihre Überwachung und Verwaltung sowie eine angemessene Aufsicht.

Zunehmende Nutzung von Anwendungen mit hartcodierten Zugangsdaten

Die Integration von COTS-Ausrüstung und IoT-Geräten in die Verkehrsinfrastruktur hat zu einem Anstieg der Nutzung von Anwendungen und Geräten mit hartcodierten Zugangsdaten geführt. Dies birgt ein erhöhtes Risiko für Kompromittierung und unbefugten Zugriff auf das Gesamtsystem. In vielen Fällen können diese hartcodierten Zugangsdaten aus der Ferne ausgelesen und genutzt werden, um physische Geräte zu manipulieren, beliebige Codes auszuführen oder Denial-of-Service-Angriffe durchzuführen.

Nutzung gemeinsamer Konten

Künftig werden die meisten Softwareanwendungen im Verkehrssektor auf COTS- oder IoT-Technologien laufen, mit deutlich geringerer Sicherheit als in den herkömmlichen IT-Umgebungen. Dies wird durch die übermäßige Nutzung gemeinsamer Konten deutlich, was für viele Unternehmen Haftungsrisiken begründet. Wenn gemeinsame Konten weit verbreitet sind, ist es sehr schwierig für ein Unternehmen, Benutzern bestimmte Aktivitäten zuzuordnen und die Handlungen mehrerer Personen zu erfassen, egal ob intern oder extern.

Fehlende Transparenz von Benutzern mit Remote-Zugriff

Angesichts der spezifischen Fähigkeiten, die für den Support und die Verwaltung der zunehmend vernetzten Systeme in einer Betriebstechnologie-Umgebung (Operational Technology; OT) erforderlich sind, lassen sich viele Industrieunternehmen durch Remote-Anbieter unterstützen. Dies umfasst auch Remote-Sessions, die mitunter tage- oder wochenlang ungesichert und ohne Überwachung andauern und die Gefahr einer Kompromittierung des gesamten Steuerungssystems bergen.

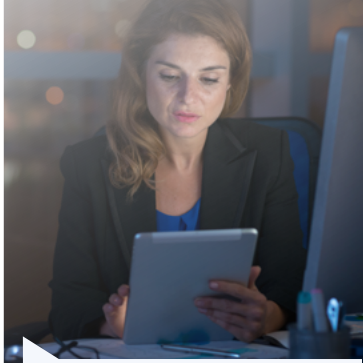
#1 HAUPTURSACHE FÜR SICHERHEITSVERLETZUNGEN: MISSBRAUCH VON PRIVILEGIERTEM ZUGANG

Schadsoftware-gebundene Spear-Phishing-E-Mails und die Verwendung von kompromittierten Remote-Zugriffs-Anmeldedaten bleiben das beliebtestes und häufigste Mittel, mit denen Malware auf wichtigen IT-Systemen der Opfer installiert wird. Insbesondere Remote Desktop Protocol (RDP) und Virtual Network Computing (VNC)-Anmeldedaten bieten Cyberkriminellen die Möglichkeit, sowohl einen ersten Zugang zu den Netzwerken zu erhalten als auch sich seitlich zu bewegen, ein wesentlicher Prozess zur Identifizierung der Systeme, auf denen Schadsoftware installiert werden sollte. Privileged Accounts und der Zugriff, den sie bieten, stellen die größten Sicherheitslücken dar, denen Unternehmen heute ausgesetzt sind. Warum konzentrieren sich Angreifer innerhalb und außerhalb des Netzwerks auf Privileged Accounts? Ganz einfach, weil Privileged Accounts überall in im Technologiestapel von Verkehrssystemen vorhanden sind.

- Erforderlich für alle vernetzten Geräte, Datenbanken, Anwendungen und On-Premise-Server, in Cloud- und ICS-Umgebungen sowie über die DevOps-Pipeline.
- Wird sowohl von Menschen als auch von maschinellen Benutzern verwendet und gewährt einen allmächtigen Zugriff auf vertrauliche Daten und Systeme.
- Haben gemeinsamen Administrator-Zugriff und machen ihre Benutzer anonym.
- Gewährung zu breiter Zugriffsrechte, die weit über das hinausgehen, was der Benutzer zur Erfüllung seiner Aufgaben benötigt.
- Oftmals unkontrolliert und nicht gemeldet und damit ungesichert.

Die Rolle der privilegierten Accounts

Privilegierte Accounts finden sich in jeder Software auf einem Netzwerk sowie in vielen Hardwaregeräten und können jeder Person, die im Besitz privilegierter Anmeldedaten ist, den Zugriff auf und die Kontrolle über sensible Daten oder kritische Systeme ermöglichen. Diese Konten erlauben den Zugriff auf wichtige Ressourcen wie Bedienstationen, um automatisierte Prozesse zu starten, Systeme zu verwalten, Parameter von Herstellungsprozessen zu ändern und historische Daten zu speichern sowie weitere wichtige Vorgänge durchzuführen. In den falschen Händen können diese Konten jedoch für den unbefugten Zugriff auf das ICS genutzt werden und damit irreparable Schäden verursachen. Dennoch sind sich einige Unternehmen der Risiken, die nicht verwaltete privilegierte Accounts für das Geschäft darstellen, nicht bewusst.



Bei der überwiegenden Mehrheit der Cyberangriffe sind kompromittierte Privileged Accounts und Anmeldedaten beteiligt.

UNTERSCHÄTZEN SIE IHR RISIKO?

- In unserem jüngsten Bereicht CyberArk Threat Landscape 2018 haben wir festgestellt, dass 89 Prozent der für IT-Sicherheit Verantwortlichen einräumten, dass IT-Infrastruktur und kritische Daten nicht vollständig geschützt sind, wenn Privileged Accounts und Anmeldedaten nicht besonders gesichert werden.
- Trotzdem gab ein größerer Teil der Befragten an, noch keine Sicherheitslösung für Privileged Accounts implementiert zu haben, um privilegierte und/oder administrative Passwörter zu speichern und zu verwalten.
- Aus dem Bericht geht auch hervor, dass Unternehmen nicht genug zum Schutz vor Malware und Angriffen mit ausgefeilten Methoden unternehmen. 87 Prozent der Befragten gaben jedoch an, dass sie weiterhin für Benutzer lokale Administratorberechtigungen zulassen. Wie allgemein bekannt erfordert die meiste Malware Administratorzugriff, um ihre Schadwirkung zu entfalten.
- Durch die Kombination von Benutzerkonten, die über lokale Administratorberechtigungen verfügen, mit den von tatsächlichen Administratoren entsteht eine ständig wachsende Angriffsfläche für privilegierte Accounts.

> **Moderne Verkehrssysteme sind in hohem Maße von einer Vielzahl von IT-Systemen abhängig und daher natürlich durch ein breites Spektrum von Cyberbedrohungen gefährdet. Cyberangriffe können die physischen Systeme eines Verkehrsbetriebs beschädigen, sie funktionsunfähig machen, die Kontrolle über diese Systeme an Unbefugte übergeben oder die Vertraulichkeit von Mitarbeiter- oder Kundendaten gefährden."**
>
> Quelle: American Public Transit Association

ERSTELLUNG EINES AKTIONSPLANS

Eine der effektivsten Vorbeugemaßnahmen, die ein Verkehrs- oder Infrastrukturunternehmen in seinem Programm zur Cybersicherheit vorsehen kann, ist die Sicherung seiner Privileged Accounts, Anmeldedaten und Geheimnisse. Entscheidungsträger der Cybersicherheit erkennen an, dass der Prozess vor allem in großen Unternehmen komplex werden kann, und die Sicherung des privilegierten Zugriffs ist leider keine einmalige Angelegenheit. Denn die Angreifer suchen unermüdlich nach Schwachstellen in Unternehmen. So mag beispielsweise ein Unternehmen vor einem Jahr den privilegierten Zugriff gesichert haben. Aber inzwischen kann es eine neue Infrastruktur, neue SaaS-Anwendungen oder mit DevOps-Methoden erstellte Anwendungen geben, ein erweitertes Cloud-Portfolio oder eine geplante Konsolidierung des Rechenzentrums. Um den stärksten Schutz vor Angreifern zu gewährleisten, müssen Unternehmen sicherstellen, dass ihr Programm für privilegierte Zugriffssicherheit aktuell ist und weiterhin ihre kritischste Infrastruktur, Anwendungen, Kundendaten, geistiges Eigentum und andere wichtige Vermögenswerte schützt.

Um das Risiko für den privilegierten Zugriff von Angreifern proaktiv zu reduzieren, müssen Unternehmen aus dem Transport- oder Verkehrswesen normalerweise Folgendes tun:

- Nutzen Sie ihr Verständnis für die häufigsten Arten von Angriffen, die den privilegierten Zugriff ausnutzen: Wie denkt und handelt ein Angreifer in jedem Fall, um die Schwachstellen des Unternehmens auszunutzen?
- Priorisieren Sie die wichtigsten Privileged Accounts, Anmeldedaten und Geheimnisse und identifizieren Sie die potenziellen Schwächen und Schwachstellen in ihrem bestehenden Sicherheitsprogramm für privilegierten Zugriff, insbesondere diejenigen, die kritische Infrastrukturen, die Kronjuwelen des Unternehmens usw. gefährden könnten.
- Die wirksamsten Maßnahmen bestimmen, um diese Schwachstellen und potenziellen Sicherheitslücken zu beheben. Welchen Maßnahmen kommt die höchste Priorität zu? Was kann man schnell erreichen im Vergleich zur Notwendigkeit eines längerfristigen Plans?
- Sicherstellung einer kontinuierlichen, erneuten Bewertung und Verbesserung der Hygiene für privilegierten Zugriff, um einer sich ändernden Bedrohungslage zu begegnen.

PRIVILEGED-ACCOUNT-DATEN
DER SCHLÜSSEL ZUM UNTERNEHMEN

- Privilegierte Anmeldedaten sind ein so wichtiges Element im IT-Betrieb, dass sie für den Zugriff auf und die Freischaltung von Privileged Accounts erforderlich sind, und sie werden von externen Angreifern und böswilligen Insidern gesucht, um direkten Zugriff auf das Herz des Unternehmens zu erhalten. Deshalb sind geschäftskritische Systeme und sensible Daten nur so sicher wie die privilegierten Anmeldedaten, die für den Zugriff auf diese Ressourcen benötigt werden.
- Die meisten Unternehmen heutzutage vertrauen auf eine Kombination aus privilegierten Anmeldedaten wie Passwörtern, API-Keys, Zertifikaten, Token und SSH-Keys zur Authentifizierung von Benutzern und Systemen für Privileged Accounts. Wenn sie ungesichert bleiben, können Angreifer diese wertvollen Geheimnisse und Anmeldedaten kompromittieren, um sich Privileged Accounts zu sichern und sie für Angriffe gegen Unternehmen zu nutzen. Studien zur Cyber-Sicherheit belegen, dass der erfolgreiche Zugriff auf einen Privileged Account die gemeinsame Grundvoraussetzung aller erfolgreichen Cyber-Angriffe ist.
- Um gezielte Angriffe zu verhindern, die Schlüssel zum IT-Königreich zu schützen und sensible Daten von Angreifern fernzuhalten, müssen Unternehmen eine Strategie der privilegierten Zugriffssicherheit verfolgen, die einen proaktiven Schutz und die Überwachung aller privilegierten Geheimnisse und Anmeldedaten beinhaltet.

CYBERARK:
IHR PARTNER FÜR CYBERSICHERHEIT IM BEREICH TRANSPORT & VERKEHR

Unabhängig davon, ob Sie native oder traditionelle Cloud-Anwendungen ausführen, die On-Premise, in der öffentlichen Cloud oder in hybriden Umgebungen ausgeführt werden, konzentriert sich CyberArk weiterhin darauf, die Angriffskette für privilegierte Zugriffssicherheit zu durchbrechen. Kürzliche Studien haben gezeigt, dass 76 bis 80 Prozent aller Sicherheitsverletzungen mit privilegierten Anmeldedaten verbunden sind. Und diese privilegierten Anmeldedaten können von böswilligen Insidern und externen Hackern gleichermaßen gefährdet werden. Mit CyberArk können Einzelhandelsunternehmen Angreifer davon abhalten, Daten zu stehlen und den Betrieb zu stören, indem sie den privilegierten Angriffspfad blockieren. Erfahren Sie, warum sich weltweit öffentliche und private Verkehrs- und Transportunternehmen auf CyberArk verlassen, um die Risiken von Angriffen zu minimieren. Wenden Sie sich an uns oder besuchen Sie www.cyberark.de.

CyberArk bleibt der unangefochtene Marktführer im Markt für privilegierte Zugriffssicherheit. Deshalb vertrauen mehr als die Hälfte der Fortune-500-Unternehmen auf CyberArk, um ihre wichtigsten und hochwertigsten Assets zu schützen. Um mehr zu erfahren, besuchen Sie uns unter www.cyberark.com/de.

05.19. Doc. CyberEdge003