DriveLock
securing your digital tomorrow

Schutz Kritischer Infrastrukturen

Whitepaper

Autoren: Oliver Rolofs, Founder & Managing Partner der Münchner Kommunikations- und Strategieberatung COMMVISOR
und Andreas Fuchs, Director Product Management, DriveLock SE

Inhalt

DriveLock
securing your digital tomorrow

Wenn sich immer mehr auf digitale Technologien verlassen wird, wachsen auch die Risiken, dass ein großangelegter Cyberangriff auf kritische Infrastrukturen Staat und Gesellschaft in ein Chaos stürzen kann. Ist Deutschlands Cybersicherheitsarchitektur für diese Bedrohungslage richtig aufgestellt? Wie können unsere lebenswichtigen kritischen Infrastrukturen besser geschützt werden?

Die Nutzung mobiler Geräte, die zunehmende Vernetzung der IT-Systeme oder Cloud-Lösungen, bringen nicht nur Vorteile für die wirtschaftliche Entwicklung und die Verbesserung unserer Lebensbedingungen mit sich, sondern auch eine Reihe neuer Herausforderungen. Nahezu alle kritischen Infrastrukturbereiche (KRITIS), ob Finanzwesen, Energie- oder Gesundheitsversorgung sind heute von der Informationstechnologie abhängig. Diese Abhängigkeit macht schützenswerte Assets anfällig für Angriffe und stellen somit eine Bedrohung dar.

Dass die Digitalisierung nicht nur Segen bringt, musste im Sommer 2021 die Verwaltung des Landkreises Anhalt-Bitterfeld erfahren. Sie wurde Opfer eines Ransomwareangriffs und rief bundesweit erstmals einen „Cyber-Katastrophenfall" aus. Auch über ein Jahr später kämpft die Kommune in Sachsen-Anhalt mit den Nachwirkungen dieser schweren Hackerattacke. Auch international gab es im letzten Jahr gravierende Vorfälle, wie die Beispiele beim amerikanischen Pipelinebetreiber Colonial Pipeline oder der irischen Gesundheitsbehörde zeigen. Keine Woche vergeht, in der Unternehmen oder Organisationen nicht Opfer von Malware- oder Ransomwareattacken werden. Eine aktuelle Studie[1] des Big-Data-Spezialisten Splunk zeigt etwa, dass die schnellste Ransomware-Bedrohung, LockBit, in weniger als sechs Sekunden verschlüsseln kann.
Besorgniserregend ist, dass Bedrohungsakteure zunehmend öffentliche Einrichtungen wie Stadtwerke sowie Lieferketten ins Visier nehmen. Die nächste Attacke ließ auch nicht lange auf sich warten: Im Juni 2022 wurde ein IT-Dienstleister aus Hessen Opfer eines Ransomwareangriffs[2], von dem schließlich auch Energieversorger und Verkehrsbetriebe im Frankfurter Raum, Darmstadt und Mainz betroffen waren, nachdem sie diverse digitale Dienstleistungen an das attackierte Unternehmen ausgelagert hatten. Zwar war die Energieversorgung sichergestellt und auch Busse und Bahnen fuhren. Doch vom Fahrscheinverkauf, der Anzeige von Fahrplänen bis hin zum Zugriff auf betreffende Webpages, E-Mail-Konten von Mitarbeitenden und Online-Dienstleistungen ging tagelang gar nichts mehr. Die Corona-Pandemie bedingte Umstellung auf das Arbeiten von zu Hause hat dabei die Angriffsfläche von Unternehmen und Behörden nochmals vergrößert. Die Zahlen zeigen, dass sich Cyberkriminalität zu einer Parallelpandemie entwickelt hat und konventionelle Sicherheitsmechanismen immer weniger greifen. Der Bitkom e. V. schätzt den verursachten Schaden durch Cyberkriminalität[3] allein in Deutschland auf inzwischen 203 Milliarden Euro pro Jahr. Das vermehrte Auftreten von digitaler organisierter Kriminalität oder staatlichen Hackergruppen potenziert die Cybergefahren und das Schadenspotenzial um ein Vielfaches.

[1] https://www.splunk.com/en_us/blog/security/gone-in-52-seconds-and-42-minutes-a-comparative-analysis-of-ransomware-encryption-speed.html
[2] https://www.heise.de/news/Ransomware-Angriff-auf-hessischen-IT-Dienstleister-mit-weitreichenden-Folgen-7140974.html
[3] 203 Milliarden Euro Schaden pro Jahr durch Angriffe auf deutsche Unternehmen | Bitkom e. V.

Cyberangriffe neue Normalität

Die neue Realität ist, dass die meisten kritischen Infrastrukturen wie Strom, Verkehr und das Gesundheitssystem in einer digitalen Umgebung arbeiten, die über das Internet zugänglich ist. Derartige Systeme bieten eine Vielzahl möglicher Angriffsvektoren, über welche beispielsweise die Verfügbarkeit der Infrastruktur beeinträchtigt werden kann oder sensible Daten gestohlen bzw. manipuliert werden können.

Die Abwehr von Angriffen auf diese Kritischen Infrastrukturen ist eine ständig wachsende Herausforderung. Laut dem Global Risks Report 2020[4] des Weltwirtschaftsforums (WEF) sind Cyberangriffe auf Kritische Infrastrukturen in Sektoren wie Energie, Gesundheitswesen und Verkehr zur neuen Normalität geworden. Denn mit der steigenden Vernetzung steigt auch die Zahl der Cyberangriffe gegenüber Staat und Wirtschaft. Besonders gezielte Angriffe und sogenannte "Advanced Persistent Threats" (APT) bedeuten eine enorme Bedrohung für IT-Systeme in Kritischen Infrastrukturen. Hinter diesen Angriffen stecken meist größere Organisationen bis hin zu Regierungen, die umfangreiche Ressourcen für die Entwicklung von Schadcodes besitzen. Der Sommer 2022 war etwa von den drei Top-Bedrohungen Software Vulnerabilities, Ransomware- und Phishingattacken geprägt, die mit Erfolg ihr Ziel fanden: Unternehmen und ihre Mitarbeiter und dabei im wachsenden Maße auch kommunale Betreiber mit Schnittstellen zu kritischen Infrastrukturen.
Gerade der Einsatz von Ransomware und der anschließenden Erpressung von Geld zur Wiederfreigabe der Daten hat sich für Cyberkriminelle als lukrativ erwiesen, wenn Betroffene darauf eingegangen sind, wovon immer abzuraten ist.

Wachsende Komplexitäten, veraltete Systeme, hohes Stresslevel für IT-Sicherheitskräfte

Erschwerend kommt hinzu, dass sich die Komplexität der IT-Umgebung in den letzten Jahren in jeder Organisation dramatisch erhöht hat. Der Umstieg von einer zentralisierten IT in dezentral verwaltete Cloudlösungen ist im vollen Gange. Unzählige Cloud-Applikationen führen zu einer noch dichteren Vernetzung und vielen neuen Schnittstellen, die spätestens seit der Corona-Pandemie durch mobiles Arbeiten oder das Arbeiten von zuhause noch mal zu einer Vielzahl neuer Zugänge ins Unternehmensnetzwerk geführt haben und die Sicherheitsperimeter verändern.

Das setzt IT-Sicherheitskräfte unter Stress und bereitet ihnen schlaflose Nächte, gerade im öffentlichen Sektor, wo viele Stellen aufgrund des Fachkräftemangels im IT-Bereich seit längerem nicht besetzt sind. Und viel schlimmer: Knapp die Hälfte der in einem jüngst veröffentlichten „Voice of SecOps"-Report des IT-Sicherheitsspezialisten Deep Instinct befragten IT-Sicherheitsverantwortliche erwägt gar, die Branche zu verlassen.[5] Der Hauptgrund ist ein „erhöhtes und untragbares Stressniveau". Doch auch andere Faktoren machen den Chief Information Security Officers (CISOs) und ihren Mitarbeitern das Leben zunehmend schwer: beispielsweise die sich weiterentwickelnden Taktiken bösartiger Akteure, der erhebliche Mangel an Cyber-Kenntnissen und verfügbaren Experten sowie bei einer gar drohenden Rezession die Entlassung von Mitarbeitenden, die versehentlich oder vorsätzlich sensible Unternehmensdaten mitnehmen.
CISOs müssen sich nicht nur um die Sicherheit des eigenen Unternehmens kümmern, sondern auch dafür sorgen, dass alle ausgelagerten Anbieter und Drittparteien, die mit ihrem Unternehmen verbunden sind, über das gleiche Sicherheitslevel verfügen und als verlässlich gelten.[6]

[4] https://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf
[5] https://www.deepinstinct.com/news/the-great-resignation-reaches-the-cybersecurity-industry
[6] https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_005.pdf

Was ist zu tun?

Die aktuellen Regulierungen geben hier eine notwendige Hilfestellung, etwa das KRITIS-Gesetz[7] oder die europäische NIS-2-Richtlinie[8], um geeignete Sicherheitsmaßnahmen auf- und auszubauen. Gut ist etwa, dass die NIS-2-Richtlinie die Sicherheitsanforderungen an Organisationen und Unternehmen verschärft und sich auch mit der Sicherheit von Lieferketten und den Beziehungen zwischen Anbietern befasst. Gerade hier liegen noch viele unkontrollierte Einfallstore, die es zu schließen gilt.

Für CISOs in Organisationen ist es zudem entscheidend, eine Strategie zu entwickeln, die Cybersicherheit vereinfacht und kontrollierbarer macht. Und sie die Sicherheitstools und -prozesse bei der Hand haben, die ihnen dabei helfen können, die aktuelle Bedrohungslandschaft zu bewältigen und gleichzeitig die Vorschriften einzuhalten. Eine dieser Lösungen ist gerade mit Blick auf unübersichtliche IT-Umgebungen und Cloud-Lösungen der umfassende Einsatz von Endpoint Security, um die verschiedenen Endgeräte in einem Netzwerk vor diversen Bedrohungen zu schützen. Technische und organisatorische Maßnahmen verhindern den unbefugten Zugriff auf Geräte oder die Ausführung schädlicher Software.

Mehr koordinierte Zusammenarbeit und mehr Awareness

Die deutsche Cybersicherheitsarchitektur verteilt sich über ca. 50 Institutionen, Ressorts und Organisationen auf den Ebenen von Bund, Ländern und Kommunen und erschwert mit dieser Komplexität eine wirkungsvolle Sicherheitsstrategie. Dies führt zu einer Verantwortungsdiffusion in der effektiven Bekämpfung von Cybergefahren. Umso wichtiger ist es, nicht nur angesichts der vielen neu entstandenen Regularien für Cybersicherheit eine klare Verantwortungsstruktur zu schaffen, sondern künftig auch ein besonderes Augenmerk darauf zu legen, welche Sicherheitslösungen im Bereich der oftmals privat betriebenen Kritischen Infrastrukturen eingesetzt werden.

Entscheidend ist, dass es klar definierte Kriterien gibt, welche Sicherheitslösungen im Bereich der oftmals privat betriebenen Kritischen Infrastrukturen eingesetzt werden. Hier sollte schnell nachgesteuert werden. KRITIS-Betreiber sollten aus eigenem Interesse auf Hersteller und Lösungen setzen, die es ihnen erlauben, dass die Daten in Europa bleiben und so die Souveränität über Daten und Sicherheit zu stärken.

Bedrohungen und Gegenmaßnahmen für die Kritische Infrastruktur

Industrial Control Systems (ICS) steuern physische Prozesse und sind die Grundlage für den Betrieb in Schlüsselindustrien wie Elektrizität, Öl, Gas, Wasser, Transport, Produktion, chemische Produktion bis hin zur Fabrikautomation, Verkehrsleittechnik und modernem Gebäudemanagement.

[7] https://www.bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-und-Verordnungen/IT-SiG/2-0/it_sig-2-0_node.html
[8] https://www.consilium.europa.eu/de/press/press-releases/2022/11/28/eu-decides-to-strengthen-cybersecurity-and-resilience-across-the-union-council-adopts-new-legislation/

Das BSI nennt in seinem Bericht „Industrial Control System Security“[9] die größten Cyber-Bedrohungen, die aus Schwachstellen resultieren. Das sind:

- Einschleusen von Schadsoftware über Wechseldatenträger und mobile Systeme
- Infektion mit Schadsoftware über Internet und Intranet
- Menschliches Fehlverhalten und Sabotage
- Social Engineering und Phishing
- (D)DoS Angriffe
- Internetverbundene Steuerungskomponenten
- Einbruch über Fernwartungszugänge
- Soft- und Hardware Schwachstellen in der Lieferkette

Ausgehend von den primären Angriffen können sich Angreifer durch Folgeangriffe sukzessive im Unternehmen ausbreiten und Folgeangriffe starten.

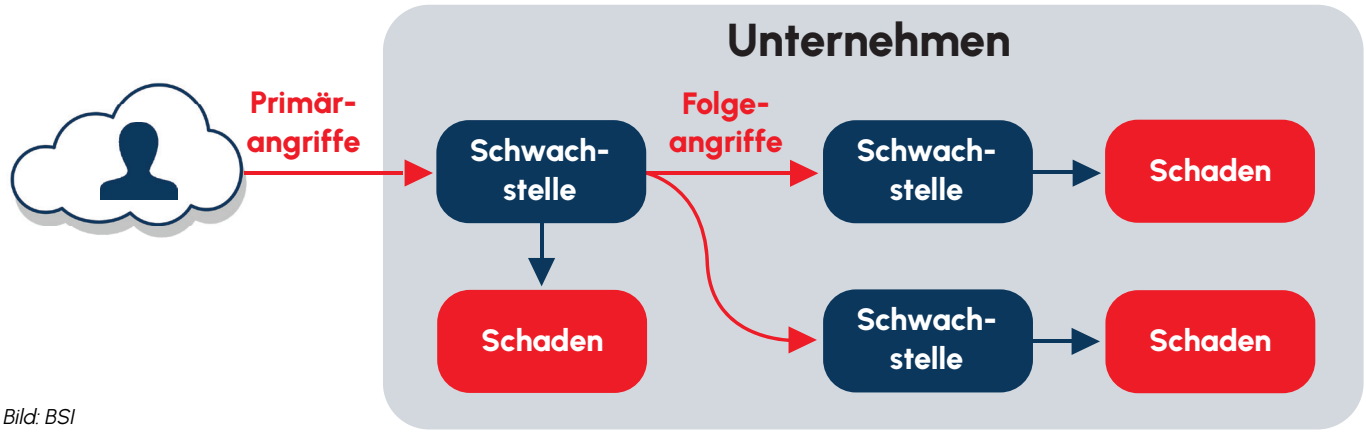


Bild: BSI

Beispiele für Folgeangriffe können Rechteerweiterungen und der Einsatz von Ransomware sein. Vorhandene IT-Standardkomponenten enthalten oft Fehler und Schwachstellen, die von Angreifern ausgenutzt werden können. Zusätzlich zum Basisschutz gegen primäre Angriffe muss der Einsatz von Kritischen Sicherheitskontrollen (CSC) erfolgen, um die Folgeangriffe zu unterbinden.
Prävention ist die effektivste Verteidigung. Die Umsetzung von Maßnahmen gegen solche Folgeangriffe sollte im Anschluss an die Etablierung eines Basisschutzes gegen die primären Angriffe und im Zuge eines sogenannten Defense-in-Depth Konzept erfolgen.
Gegenmaßnahmen zur Bekämpfung der identifizierten Bedrohungen sollten nach technischer oder organisatorischer Umsetzbarkeit bewertet werden. Nicht jede Gegenmaßnahme ist hilfreich, aber in Summe lindern sie merklich das Risiko, das von solchen Bedrohungen ausgeht.
Exemplarisch für präventive Sicherheitsmaßnahmen wird folgend der Anwendungsfall einer Gerätekontrolle beschrieben.

[9] https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_005.pdf

Einschleusen von Schadsoftware über Wechseldatenträger und mobile Systeme

Ein Erfahrungsbericht des BSI[10] schildert einen IT-Sicherheits-Zwischenfall im industriellen Umfeld. In einer verteilten Infrastruktur eines Betreibers ist es in mehreren Leitstellen vermutlich zu einem Virenbefall gekommen. Das Papier gehört zu einer Reihe von Erfahrungsberichten, mit denen häufig beobachtete Probleme im ICS-Umfeld aufgezeigt werden. Eine der häufigsten Infektionsquellen für Viren oder Malware in industriellen Umgebungen ist die Verwendung eines USB-Geräts, das unwissentlich infiziert ist. Wechseldatenträger gehören zu den gängigen Angriffsmethoden, denn sie haben sich zu den Haupteinstiegspunkten für Angriffe entwickelt, da diese Komponenten häufig missbraucht werden, um Schadsoftware und bösartige Befehle auf die Systeme zu laden oder sensible Informationen auszulesen. Deshalb muss die Nutzung von Wechseldatenträgern und mobilen Geräten kontrolliert und eingeschränkt werden durch die konsequente Anwendung von Gerätekontrolle.
Mit dieser können Laufwerke und Geräte überwacht und explizit aktiviert oder deaktiviert werden. In ICS/OT-Umgebungen sollten alle externen Schnittstellen standardmäßig blockiert werden. Wechseldatenträger können z. B. im Office-Netz oder im privaten Umfeld infiziert worden sein. Schadsoftware kann so ihren Weg direkt in die ICS-Netze finden. Aber auch Wartungsnotebooks können beim Zugriff auf das Internet, in Office-Netzen oder in der Infrastruktur des jeweiligen externen Dienstleisters infiziert werden. Sobald diese dann im ICS-Netz betrieben werden, erfolgt die Infektion der dortigen Systeme und Komponenten mit Schadcode.
Bei Diebstahl oder Verlust von mobilen Datenträgern mit sensiblen Informationen ist die Gefahr groß, dass z. B. Passworte oder vorkonfigurierte Zugänge ins ICS-Netz in falsche Hände geraten. Als Maßnahme hilft hier die automatische Verschlüsselung der Daten auf externe Speichermedien. Somit sind die Daten vor Zugriff geschützt.
Vorbeugende Maßnahmen sind u. a.:

- Inventarisierung und Whitelisting zugelassener Wechseldatenträger.
- Wechseldatenträgerschleuse mit integriertem Virenschutz. Steckt man sie an, werden sie vor Freischaltung auf Viren geprüft.
- Ausschließliche Verwendung unternehmenseigener oder personalisierter Wechseldatenträger.
- Verschlüsselung der Datenträger.

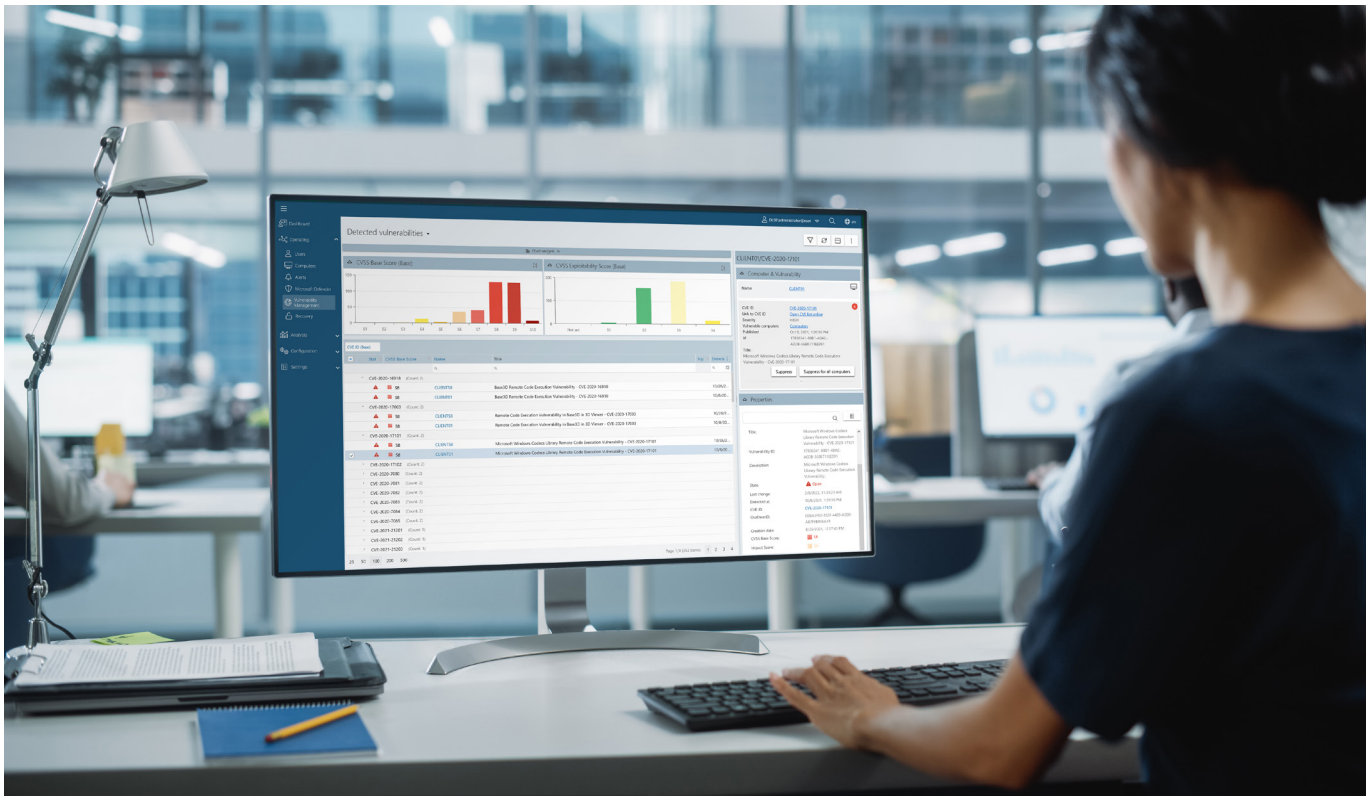
Ergänzende Sicherheitsmaßnahmen

ICS-Anlagenbetreiber sollten ein funktionierendes Informationssicherheitsmanagement (ISMS) auf Basis etablierter Standards aufbauen, die sowohl allgemein bzgl. IT-Sicherheit als auch spezifisch zur ICS-Sicherheit Vorgaben enthalten.
Neben den oben genannten Sicherheitskriterien lohnt sich der Blick in die etablierten Standards wie IT-Grundschutz[11], ISO 27000 Reihe[12], NIST Cybersecurity Framework[13], VDI/VDE 2182[14], IEC 62443[15] et al.

[10] https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_095c.pdf
[11] https://www.bsi.bund.de/IT-Grundschutz
[12] https://www.iso.org/isoiec-27001-information-security.html
[13] https://www.nist.gov/cyberframework
[14] https://www.vdi.de/richtlinien
[15] https://www.iec.ch/cyber-security

Effektiver Schutz für Industrieanlagen mit Security aus der Cloud

Um die empfohlenen präventiven Maßnahmen mit eigenem Personal stemmen zu können, d.h. die Lösungen einzuführen und zu betreuen, braucht es Investitionen in Mitarbeiter, Ausbildung und Systeme. Der Fachkräftemangel ist hier nur eines von mehreren Hindernissen. Diese Rahmenbedingungen können dazu führen, dass Security-Lösungen zwar initial eingerichtet und konfiguriert werden, es aber im laufenden Betrieb keine weiteren Anpassungen mehr gibt. Dadurch sinkt das Sicherheitsniveau mit der Zeit. Eine Alternative ist, die IT-Lösungen von einem Servicedienstleister managen zu lassen. Namhafte Dienstleister bieten ihre Lösungen zum Schutz von Endpoints als Managed Security aus der Cloud an. Sie stellen ein umfängliches fertig konfiguriertes Sicherheitsprofil zur Verfügung, das auf den jeweiligen Lösungsmodulen basiert. Der Schutz der Endgeräte ist sofort verfügbar. Darüber hinaus werden diese Sicherheitsprofile permanent weiterentwickelt und an aktuelle Bedürfnisse angepasst und optimiert. Weitere Vorteile dieser Cloud-basierten Endpoint-Security Lösungen sind die Kostenkontrolle, eine schnelle Bereitstellung sowie automatische Updates, sowie vordefinierte und auf den Industriezweig angepasste Sicherheitsrichtlinien. Unternehmen haben keine zusätzlichen Investitionen in Hardware und genießen höchsten Schutz für Ihre Daten.



Über DriveLock

Das deutsche Unternehmen DriveLock SE wurde 1999 gegründet und ist inzwischen einer der international führenden Spezialisten für Cloud-basierte Endpoint- und Datensicherheit mit Repräsentanzen in Deutschland, Australien, Singapur und USA.

In Zeiten der digitalen Transformation hängt der Erfolg von Unternehmen maßgeblich davon ab, wie zuverlässig Menschen, Unternehmen und Dienste vor Cyberangriffen und vor dem Verlust wertvoller Daten geschützt sind. DriveLock hat es sich zum Ziel gesetzt, Unternehmensdaten, -geräte und -systeme zu schützen. Hierfür setzt das Unternehmen auf neueste Technologien, erfahrene Security-Experten und Lösungen nach dem Zero Trust Modell. Zero Trust bedeutet in heutigen Sicherheitsarchitekturen einen Paradigmenwechsel nach der Maxime **„Never trust, always verify"**. So können auch in modernen Geschäftsmodellen Daten zuverlässig geschützt werden.

Die DriveLock Zero Trust Plattform vereint die Elemente

- Data Protection
- Endpoint Protection
- Risk & Compliance
- Identity & Access Management

Cloud-basierte Lösungen von DriveLock bieten mehrschichtige Sicherheit; sie sind sofort verfügbar und wirtschaftlich effizient mit niedrigen Investitionskosten. Die DriveLock-Lösungen Device Control und Application Control sind nach Common Criteria EAL3+ zertifiziert: Mit dieser international anerkannten Zertifizierung werden die hohe Vertrauenswürdigkeit und der Sicherheitsstandard des DriveLock Agents attestiert.

DriveLock ist Made in Germany und „ohne Backdoor".

Mehrere Millionen verwaltete Endgeräte in 30 verschiedenen Ländern

Kundenumgebungen mit über 180.000 verwalteten Endgeräten

Made in Germany: Entwicklung und technischer Support aus Deutschland

Kontaktieren Sie uns!

DriveLock SE
+49 (89) 546 36 49-0
info@drivelock.com

www.drivelock.com