WHITE PAPER

DIE SICHERE NUTZUNG VON USB-LAUFWERKEN IN INDUSTRIELLEN UMGEBUNGEN

In diesem Beitrag werden die Risiken bei der Nutzung von USB Speichern in einem industriellen Umfeld aufgezeigt und eine sichere Lösung vorgestellt. Diese dient in Kombination mit einem mehrschichtigen Sicherheitsansatz dazu, industrielle Steuerungssysteme zu schützen. Dabei ist das Ziel die Verbesserung der Sicherheit, Zuverlässigkeit und Verfügbarkeit der Steuerungssysteme, sowie der Schutz vor physischen, wirtschaftlichen und sozialen Auswirkungen infolge von industriellen Sicherheitslücken.

EINFÜHRUNG IN USB-SICHERHEITS-ASPEKTE IN INDUSTRIELLEN STEUERUNGSSYSTEMEN

Eine Schadsoftware, die das Institut MIT als die mörderischste Malware der Welt bezeichnet und die erstmals aufgetreten ist, als sie eine petrochemische Anlage im Nahen Osten zur Explosion gebracht hat, verbreitet sich Berichten zufolge nun in Nordamerika und im Rest der Welt. Dies geschieht zu einer Zeit, in der weltweit mehr als 2,5 Millionen Industrieroboter in Branchen wie Automobil, Elektrik/Elektronik, Metall/Maschinen, Kunststoffe/Chemikalien bis hin zu Lebensmitteln und Getränken im Einsatz sind.[1]

Diese Maschinen und die dort angeschlossenen Systeme sind üblicherweise mit der omnipräsenten USB-Schnittstelle ausgerüstet, die wir alle so gut von unseren Desktop-PCs kennen. Der USB-Anschluss bietet Möglichkeiten für Wartung, Statistiken und vieles mehr, erfordert jedoch auch Verfahren und Maßnahmen, um die Organisationen, die sie verwenden, zu schützen. Und über die bekannt gewordenen Angriffe hinaus, steht viel auf dem Spiel, wie dieses Zitat von IT-Sicherheitsforschern[2] im amerikanischen Wired Magazin bezüglich eines typischen USB-Angriffs zeigt:

> *"Physische Sabotage: Das Manipulieren eines Industrieroboterarms kann Fehlproduktionen im Wert von mehreren Millionen Dollar zur Folge haben und möglicherweise der Maschine oder sogar ihrem menschlichen Bediener Schaden zufügen."* [3]

Zusätzlich zu den Industriezweigen, in denen Roboter eingesetzt werden, gibt es viele Branchen, die sich auch auf OT- (Operational Technology) Netzwerke verlassen und in hohem Maße auf den USB-Anschluss angewiesen sind. Zu den technologie-intensiven Branchen gehören Öl und Gas, Strom und Versorgung, Herstellung von Chemikalien, Wasseraufbereitung, Abfallwirtschaft, Transport, Wissenschaft, kritische Fertigung, Gebäudemanagement und -automatisierung, sowie die Steuerung und Automatisierung von Gebäudebeleuchtungen.

Diese OT-Netzwerke werden oft ganz oder teilweise aus dem IT-Netzwerk ausgelagert, um zu verhindern, dass Online-Bedrohungen in diese Bereiche eindringen können. Viele Sicherheitsstandards und Zertifizierungen wie ISO 27001 verlangen, dass die Trennung zwischen IT-Netzwerken und OT-Netzwerken kontrolliert gehandhabt wird. Die OT-Netzwerke enthalten ICS (Industrielle Steuerungssysteme), die häufig als SCADA- (Supervisory Control And Data Acquisition) System / Netzwerk oder als DCS (Distributed Control System) strukturiert sind. Diese enthalten dann Roboter, SPS-Geräte (Speicherprogrammierbare Steuerungen) und IIoT-Geräte (Industrial Internet of Things), die möglicherweise Daten über eine USB-Massenspeicherschnittstelle empfangen oder ausgeben müssen.

Elektro- und Gerätetechniker bei der Fehlerbehebung an einer programmierbaren Steuerung eines Öl- und Gasförderungssystems, Arbeiter auf einer Offshore-Ölplattform.

USB-SICHERHEITS-HERAUSFORDERUNGEN

Die Standard-USB-Massenspeicherschnittstelle an sich bietet nur sehr begrenzte Möglichkeiten die Sicherheit zu gewährleisten. Ein USB-Gerät, das sich gemäß dem USB-Standard zu erkennen gibt, erhält im Allgemeinen einen vollen Zugriff auf die Teile des Host-Systems, die von der Art des Geräts vorgegeben werden,[4] sei es als Massenspeichergerät oder als Tastatur. So wird z. B. auch der Angriff ermöglicht, der als BadUSB- oder USB-Killer bezeichnet wird und den wir jetzt genauer anschauen wollen. Doch bevor wir fortfahren, unterteilen wir zunächst die Angriffsvarianten in Hauptkategorien.

BÖSARTIGE HARDWARE

Der Hauptakteur, der maßgeblich das Vertrauen in das USB-Protokoll verletzt hat, ist unter dem Namen BadUSB bekannt. Solche BadUSB-Geräte sind, kurz gesagt, Betrüger. Sie geben sich als vertrauenswürdige Laufwerke zu erkennen, führen jedoch tatsächlich eine böswillige Attacke, häufig in Form eines Keystroke-Injection-Angriffs, aus. Das Aushängeschild für diese Art von Angriff ist der von Hak5 produzierte RubberDucky.[5] Theoretisch könnte sogar der Yubikey so programmiert werden, dass dadurch ein bösartiger Inhalt übertragen werden kann.[6] Dies sind keineswegs die einzigen Übeltäter, da auch andere Allzweck-Computerplattformen wie Arduino[7] oder Raspberry Pi[8] verwendet werden können, um denselben Angriff zu starten. Das vom Angreifer benötigte Knowhow und Budget sind sehr gering, da vorgefertigte Angriffe für wenig Geld zu bekommen sind.

"Ein USB-Gerät erhält im Allgemeinen vollen Zugriff auf die Teile des Host-Systems, die einen Angriff erst möglich machen."

ELEKTRISCHE ANGRIFFE

Der fehlende Überspannungsschutz führt zu weiterem Misstrauen gegenüber USB-Schnittstellen, da diese einfach alles, was angeschlossen wird, mit Strom versorgen. Dieses Verhalten hat den sogenannten USB-Killer erst möglich gemacht.[9] Das Gerät verwendet die von der Schnittstelle bereitgestellte Energie zum Aufladen und entlässt dann die kumulierte elektrische Last über den USB-Port zurück in den Host. Dies verursacht eine Überspannung und häufig einen vollständigen elektrischen Ausfall des Host-Rechners. Der USB-Killer ist vergleichbar mit einem Schraubenschlüssel, der in eine sich bewegende Maschine geworfen wird. Er verwendet jedoch den USB-Anschluss und hinterlässt dabei weniger Spuren. Das Endergebnis ist ein defekter Roboter ohne wirklich erkennbare Ursache.

USB JUMPING MALWARE

Wie kann man ein Offline-Netzwerk böswillig beeinflussen? Für die noch unbekannten Entwickler der Malware Stuxnet war die Antwort einfach: Infiziere so viele USB-Laufwerke wie möglich und irgendwann findet die Malware ihr industrielles Zielsystem, ganz gleich, ob dafür zehn oder tausend Anläufe benötigt werden. Stuxnet wartete geduldig, bis eines Tages ein passendes Ziel erreicht wurde: der Arbeitsplatz-PC eines Ingenieurs mit Zugriff auf die SPS-Geräte in der iranischen Uran-Anreicherungsanlage Natanz. Bei dem Angriff wurden schätzungsweise 1.000 Zentrifugen zerstört.[10] Der Stuxnet-Angriff und die dazu verwendete Technologie brachten weitere ICS-spezifische Bedrohungen hervor,[11] z. B. Trisis.[12] Trisis, manchmal auch als Triton oder Hatman bezeichnet, ist in der Lage, eine Fehlfunktion im Triconex Safety Instrumented System (SIS), einer häufig eingesetzten Logiksteuerung von Schneider Electric, zu erzwingen. Diese Steuerungen werden in erster Linie zur Verwaltung der Anlagen in Kernkraft-, Öl- und Gasproduktionswerken, sowie Papierfabriken eingesetzt.[13] Diese Angriffe können außergewöhnliche Folgen haben, wie 2019 vom MIT Technology Review berichtet wurde: "Die Schadsoftware kann Sicherheitssysteme, die entwickelt wurden, um katastrophale Industrieunfälle zu verhindern, außer Kraft setzen. Sie wurde im Nahen Osten entdeckt, doch die Hacker, die dafür verantwortlich sind, haben es jetzt auch auf Unternehmen in Nordamerika und anderen Teilen der Welt abgesehen". Dies veranlasste MIT Technology Review, sie als "die mörderischste Malware der Welt" zu bezeichnen. Der Grund dafür ist ein aufsehenerregender Angriff, den TechCrunch als Versuch, "eine saudische petrochemische Fabrik in die Luft zu sprengen", zusammenfasste.

Die allgemein gültige PLC-Schwäche, die bei diesen Angriffen ausgenutzt wird, ist die fehlende Verifizierung auf der Basis von kryptografischen Signaturen, da die Geräte mehr oder weniger das verarbeiten, was ihnen angeliefert wird - vorausgesetzt, das Format ist korrekt.

In diesem Zusammenhang sollte ebenfalls beachtet werden, dass alle normalen Desktop-Computer in OT-Netzwerken natürlich mit Standard-Malware-Angriffen infiziert werden können. Ein Beispiel ist die Anfang 2020 entdeckte Ransomware Spora, die sich über generische USB-Laufwerke ausbreiten kann.[14]

EINE USB-SICHERHEITSLÖSUNG FÜR INDUSTRIELLE UMGEBUNGEN

Der Umgang mit der Sicherheit in einer ICS-Umgebung erfordert im Allgemeinen einen mehrschichtigen Ansatz, wie er vom NIST (National Institute of Standards and Technology) im Guide to Industrial Control Systems (ICS) Security empfohlen wird.[15] USB-Schutzmaßnahmen sind dabei nur ein Teil eines komplexen Schutzkonzeptes. Speziell für die Verwendung von USB-Laufwerken hat das ICS-CERT, das National Cybersecurity and Communications Integration Center, einen Leitfaden herausgegeben, der Benutzern empfiehlt, strenge Richtlinien für Unternehmens- und ICS-Netzwerke zu erstellen. Wie diese Richtlinien gestaltet werden, hängt von der jeweiligen Organisation ab. Wir stellen nachfolgend eine allgemein praktische Vorgehensweise auf der Grundlage der Richtlinien vor, die angepasst an das jeweilige Szenario eingesetzt werden kann. Das physische Layout von Anlagen und OT-Netzwerken kann sich stark unterscheiden: von der einzelnen Industrieanlage bis hin zum weitverzweigten Netzwerk eines Stromnetzbetreibers. DataLocker kann mit seinen Professional Services auf den jeweiligen Einsatzfall angepasste Konfigurationsoptionen empfehlen.

"Die Organisation der Sicherheit in einer ICS-Umgebung erfordert im Allgemeinen einen mehrschichtigen Ansatz..."

Nachstehend ist ein genereller Lösungsvorschlag zu finden, der die erforderlichen Kriterien erfüllt:

1. Standardisierung der Verwendung von vertrauenswürdigen, verwalteten und sicheren USB-Geräten für das OT-Netzwerk
2. Die Einrichtung eines strikten Grenzbereiches um das OT-Netzwerk, in welches Daten nach Möglichkeit ausschließlich über eine White Station (Kiosk) als eine Art Grenzschutz-Gerät, übertragen werden können
3. Die Installation einer USB-Port-Verwaltungssoftware auf allen Client-PCs im OT-Netzwerk
4. Sicherstellung, dass die sicheren USB-Geräte zwischen den Nutzungszyklen oder nach einem festgelegten Zeitplan bereinigt werden können
5. Scannen aller Dateien auf Malware und Überprüfung des Hashwerts von Firmware-Dateien, die für Systeme bestimmt sind, welche die Echtheit der Firmware selbst nicht überprüfen können

Wir werden uns nun jeden Teil der vorgeschlagenen Lösung genauer ansehen.

DataLocker Sentry K350

STANDARDISIERTE USB-GERÄTE IM OT-NETZWERK

Es sollten physische Sicherheitskontrollen vorhanden sein, um zu gewährleisten, dass nur ausgewählte, vertrauenswürdige, verwaltete und sichere USB-Geräte zur Verwendung im OT-Netzwerk zugelassen werden. Dadurch wird die Bedrohung durch bösartige Hardware-Angriffe und vor allem ein elektrischer Angriff ausgeschlossen. Einige OT-Netzwerke sind in Bezug darauf, welche Geräte physischen Zugang haben dürfen, schwieriger zu kontrollieren, sodass diese Vorgehensweise oft unterstützende Maßnahmen benötigt, um wirksam zu sein.

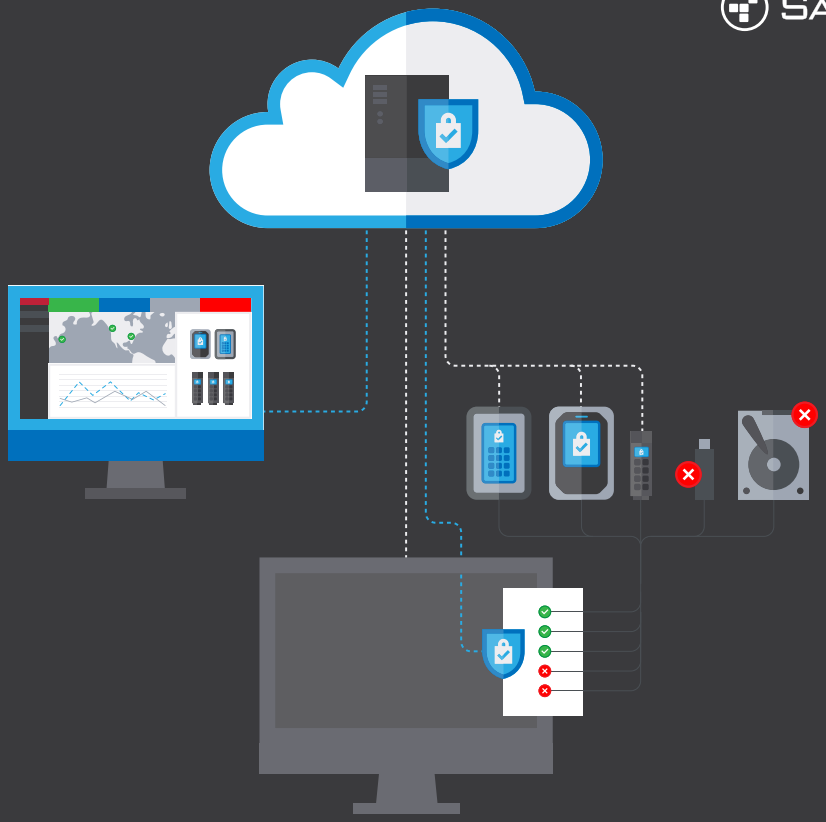
"Indem Sie den Zugriff auf den USB-Anschluss einschränken, begrenzen Sie die Bedrohung durch USB-Geräte."

DATALOCKER LÖSUNGSANSATZ

Insbesondere für OT-Netzwerke hat sich der DataLocker Sentry K350 als sehr nützlich erwiesen. Das Tastaturgerät kann vollständig verwaltet und auch überwacht werden. Wenn es an Client PCs angeschlossen wird, kann es jedoch auch als Wechselmedium mit kontrollierter, eigenständiger Authentifizierung eingesetzt werden. Die Fähigkeit zum eigenständigen Entsperren ist entscheidend, damit SPS und IoT-Geräte Daten lesen und schreiben können. Der Sentry K350 bietet auch die Möglichkeit, die Medien mithilfe einer kryptografischen Löschung zu bereinigen. Dies ist entscheidend, um die Anforderungen unterschiedlicher Netzwerke zu erfüllen. Eine kryptografische Löschung kann auch Teil einer gesetzlichen Anforderung sein, um sicherzustellen, dass vertrauliche Daten nach Abschluss eines Projektes zerstört werden.

EINRICHTUNG VON BEREICHS-SCHUTZGRENZEN

Der Zweck der Wechseldatenträgerschleuse, bzw. der White Station, besteht darin, eine Zugangskontrolle zwischen dem IT- und dem OT-Netzwerk zu implementieren. Dadurch wird für alle Daten, die in das OT-Netzwerk eingebracht werden, ein bestimmtes Sicherheitsniveau erreicht. Die White Station soll so konzipiert sein, dass sie der Wächter und das einzige Gerät ist, welches den Bedrohungen von außen begegnet. Es gibt eine Vielzahl von Möglichkeiten, einen Desktop-Computer als White Station einzurichten. Im Allgemeinen sollte das Gerät über eine aktuelle Anti-Malware-Engine und einen regelmäßigen



DataLocker PortBlocker,
verwaltet durch SafeConsole

Wartungsplan für Betriebssystem-Updates verfügen. Die Standardhardware kann beispielsweise auch durch einen ESD (Electrostatic Discharge) geschützten USB-Hub ergänzt werden, der eine Überspannung ausschließt. Es wird außerdem empfohlen, nur eine HID-Tastatur zuzulassen, um die meisten BadUSB-Gefahren umgehend zu eliminieren.

DATALOCKER LÖSUNGSANSATZ

Durch die Kombination unterschiedlicher DataLocker-Technologien ist es je nach Richtlinie möglich, eine oder mehrere White Stations einzurichten. Der DataLocker Sentry K350 kann so konfiguriert werden, dass ein integrierter McAfee-Malware-Schutz sicherstellt, dass über USB eingebrachte Malware sofort gestoppt wird. Bei der Verwaltung des DataLocker Sentry K350 ist es auch möglich, mithilfe einer Dateibeschränkungsrichtlinie vorzugeben, welche Dateitypen für das OT-Netzwerk zugelassen werden. Kombiniert man den Sentry K350 mit der Installation von der USB-Port-Kontrollsoftware PortBlocker auf einem Desktop, kann ein weiterer Schutz erreicht werden. PortBlocker kann dann so konfiguriert werden, dass ausschließlich Lesevorgänge von Geräten an der White Station zugelassen werden.

KONTROLLE DER USB-PORTS ZU JEDER ZEIT

Beschränken Sie nach Möglichkeit den Zugang zu USB-Anschlüssen an SPS- und Computergeräten durch abschließbare Schränke oder physische USB-Schlösser, wenn diese nicht mit einer USB-Port-Kontrollsoftware ausgestattet werden können. Für jedes Standardbetriebssystem sollte eine Port-Kontrollsoftware installiert werden. Die Logik hinter diesem Schutz vor Bedrohungen ist ganz einfach: Durch die Beschränkung des Zugangs zum USB-Port wird die Bedrohung durch nicht zugelassene USB-Geräte ausgeschlossen.

DATALOCKER LÖSUNGSANSATZ

Die USB-Port-Kontrollsoftware PortBlocker sollte auf allen kompatiblen Computern im OT- und IT-Netzwerk installiert werden, um sicherzustellen, dass nur die autorisierten Geräte als USB-Massenspeicher verwendet werden können.

DATENBEREINIGUNG VON SPEICHERGERÄTEN

Eine weitere sinnvolle Maßnahme um die Verbreitung von Schadsoftware zu verhindern, besteht darin, die verwendeten Speichermedien regelmäßig zu bereinigen. Dies gewährleistet zum einen saubere Kontrollpunkte im Betrieb, kann jedoch auch Teil der Einhaltung von Vorschriften sein, um nachzuweisen,

dass sensible Daten niemals unbegrenzt auf Wechselmedien gespeichert werden können. Normale USB-Laufwerke können auch als Datenhortungsgeräte bezeichnet werden, da sie so konstruiert sind, dass sie eine maximale Lebensdauer des Geräts gewährleisten. Das bedeutet, dass die Datensektoren nur dann überschrieben werden, wenn es absolut notwendig ist und unabhängig davon, ob die Dateizuordnungstabelle (FAT) ein "sauberes" Gerät anzeigt. Bei einem regulären USB-Laufwerk wiegt sich der Anwender in Sicherheit, doch die Daten können von jedermann einfach wiederhergestellt werden.

"Eine optimierte USB-Sicherheit erhöht die Sicherheit, Zuverlässigkeit und Verfügbarkeit von industriellen Steuerungssystemen."

DATALOCKER LÖSUNGSANSATZ

Hardware-verschlüsselte Laufwerke von DataLocker lösen das komplizierte Bereinigungsproblem, indem sie eine Methode namens ‚Kryptografische Löschung' verwenden. Kurz gesagt handelt es sich dabei um die Zerstörung des bisherigen, sowie die Generierung eines neuen AES-Schlüssels. Dieser Prozess stellt sicher, dass die Medien sauber sind und den NIST 800-88-Richtlinien für die Medienbereinigung (Media Sanitization) entsprechen.[16] Die meisten Länder haben ähnliche Standards wie das NIST, da eine vollständige kryptografische Löschung die schnellste und effektivste Löschung darstellt.

ANTI-MALWARE UND DATENAUTHENTIZITÄT

Die White Stations und alle kompatiblen Endpunkte im OT-Netz sollten mit mindestens einer Malwareschutzschicht ausgestattet sein, um insbesondere die Malware zu bekämpfen, die sich über USB ausbreitet. Darüber hinaus sollten alle Daten, die für PLCs oder Maschinen bestimmt sind und die selbst nicht in der Lage sind, die Daten zu validieren, auf den White Stations vorverifiziert werden. Diese Vorverifizierung kann durch die Überprüfung der kryptografischen Signaturen oder der Hashwerte erfolgen, welche vom Softwarehersteller bereitgestellt werden. Dieser Schritt stellt sicher, dass die übertragenen Daten die exakte Kopie derjenigen Daten sind, die der Softwareentwickler ursprünglich angeliefert hatte.

DATALOCKER LÖSUNGSANSATZ

Der Sentry K350 von DataLocker bietet sowohl integrierten McAfee-Malwareschutz als auch Dateitypbeschränkungen. So ist es einem Administrator möglich, den MD5-Hashwert aller auf dem Gerät gespeicherten Daten zu überprüfen, um sicherzustellen, dass nur die korrekten Daten auf die SPS übertragen werden.

DARSTELLUNG DES ANWENDUNGSSZENARIOS ZUR ERLANGUNG BESSERER USB-SICHERHEIT

In diesem White Paper wurde nachgewiesen, wie eine durchdachte USB-Sicherheitsstrategie die Sicherheit, Zuverlässigkeit und Verfügbarkeit industrieller Steuerungssysteme optimieren kann, ohne Einbußen der Produktivität hinnehmen zu müssen. Die physische Beschaffenheit der industriellen Umgebung bedeutet oft, dass das Leben, der Maschinenpark, die Produktionsleistung und die Umgebung durch Sicherheitslücken beeinträchtigt werden können. Wir haben aufgezeigt, dass die Risiken einer nicht verwalteten USB-Nutzung erheblich sein können und nicht vorsätzlich übersehen werden sollten.

Der genaue Anwendungsfall muss natürlich an das jeweilige Szenario angepasst werden und die DataLocker Partner, -Ingenieure und das Vertriebsteam beraten Sie gerne und empfehlen die für Sie passende Lösung. Auf diese Weise können wir Sie bei der Entwicklung eines gut durchdachten Implementierungs- und Kostenplans unterstützen.

Quellenangaben:

[1] https://ifr.org/downloads/press2018/Executive%20Summary%20WR%202019%20Industrial%20Robots.pdf
[2] https://robosec.org/downloads/paper-robosec-sp-2017.pdf
[3] https://www.wired.com/2017/05/watch-hackers-sabotage-factory-robot-arm-afar/
[4] https://www.usb.org/defined-class-codes
[5] https://shop.hak5.org/products/usb-rubber-ducky-deluxe
[6] https://www.blackhillsinfosec.com/how-to-weaponize-the-yubikey/
[7] https://maltronics.com/collections/malduinos
[8] https://hackaday.io/project/17598-diy-usb-rubber-ducky
[9] https://usbkill.com/
[10] https://www.cyberscoop.com/stuxnet-type-attack-airbus-cybersecurity/
[11] https://www.msp360.com/resources/blog/triton-malware/
[12] https://dragos.com/wp-content/uploads/Past-and-Future-of-Integrity-Based-ICS-Attacks.pdf
[13] https://www.cyberscoop.com/trisis-ics-malware-saudi-arabia/
[14] https://blog.knowbe4.com/alert-usb-sticks-could-infect-your-network-with-new-spora-ransomware-worm
[15] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf
[16] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

DATALOCKER

DATALOCKER B. V.
+31 467 111 205

DEUTSCH-SPRACHIGER VERTRIEBSKONTAKT:
+49 2191 437 9702

eusales@datalocker.com
Um Ihren lokalen DataLocker-Händler zu finden, besuchen Sie bitte **datalocker.com**