ZEBRA

Sicherheitsplattform
von Zebra

Schützen Sie Ihren Leistungsvorteil

Die umfassende Vernetzung, die Ihre Geschäftsabläufe beschleunigt, kann auch Sicherheitsrisiken mit sich bringen. Das Einrichten von Firewalls ist ein Anfang, reicht aber angesichts neuer und komplexer Bedrohungen nicht aus. Entdecken Sie die Best Practices und Lösungen der Enterprise-Klasse, die Ihr Unternehmen und Ihre Daten besser schützen können.

So verhindern Sie, dass Sicherheitsbedrohungen Ihr Unternehmen gefährden

Sicherheit ist unerlässlich

Kreditkartennummern. Patientenakten. Sozialversicherungsnummern. Passwörter. Ganz gleich, ob Sie Daten von Kunden, Patienten oder Bürgern verarbeiten, personenbezogene Informationen müssen vertraulich bleiben – das ist häufig sogar gesetzlich vorgeschrieben.

Risiken nehmen zu

Die Herausforderungen werden mit der Zeit immer schwieriger. Das Internet der Dinge und Cloud-Technologie ermöglichen einen beispiellosen Zugriff auf Informationen und sorgen für überragende betriebliche Kontrolle und Transparenz in Ihrem Unternehmen. Das erschließt interessante Möglichkeiten, ist aber auch mit Risiken verbunden.

Bis 2022 wird es schätzungsweise 50 Milliarden[1] vernetzte Geräte geben, was für Unternehmen und vertrauliche Daten unzählige Sicherheitsrisiken mit sich bringt. Die Motive der Angreifer sind hohe Gewinne und ein geringes Risiko (nur fünf Prozent der Hacker werden strafrechtlich verfolgt[2]), sodass es keine Anzeichen für einen Rückgang der Cyberkriminalität gibt.

Was steht auf dem Spiel?

Schon eine einzige Sicherheitslücke kann durch Produktivitäts- und finanzielle Verluste sowie Reputationsschäden hohe Kosten verursachen.

Was können Sie tun? Nehmen Sie die Sicherheit ernst. Selbst wenn Ihr Unternehmen über ein Sicherheitsprogramm verfügt, besteht die Möglichkeit, dass Fehleinschätzungen seine Integrität gefährden und unnötige Schwachstellen verursachen.

3,9 Mio. USD:
durchschnittl. Kosten einer Datenpanne[3]

25.575 Datensätze:
durchschnittl. Umfang einer Datenpanne[3]

12 Stunden:
so lange brauchen 88 % der Hacker im Schnitt, um Cybersicherheitsmaßnahmen zu durchbrechen[4]

197 Tage:
so lange dauert es durchschnittlich, bis Unternehmen einen Angriff erkennen[3]

Ziele:

Einzelhandel:
80 % der Loginversuche in Onlineshops kommen von Hackern, die gestohlene Daten verwenden[5]

Behörden/ öffentlicher Sektor:
Spionage und finanzielle Gewinne sind die Hauptmotive für Attacken[6]

Gesundheitswesen:
Mit 15 % aller Cyberangriffe die am zweithäufigsten betroffene Branche[6]

Fertigung:
In den letzten Jahren häufiger als andere vertikale Märkte von Cyberspionage betroffen[6]

Lassen Sie nicht zu, dass Fehleinschätzungen die Sicherheit schwächen

Obwohl Sicherheitsvorfälle nach wie vor für Schlagzeilen sorgen, haben viele Unternehmen ein falsches Gefühl der Sicherheit. Wiegen Sie sich nicht in trügerischer Sicherheit. Wenn Ihnen die nachstehenden Aussagen bekannt vorkommen, könnte auch Ihr Unternehmen in Schwierigkeiten sein.

„Mein Unternehmen ist nicht groß genug, um Ziel von Angriffen zu sein."

43 % der Cyberangriffe betreffen kleine Unternehmen.[6] Hacker machen sich den Mangel an Ressourcen und Wissen in kleinen Unternehmen zunutze. Sie können sogar versuchen, über Ihr Unternehmen Zugriff auf die Daten größerer Organisationen zu erhalten.

„Wir sind durch unser Netzwerk geschützt."

Eine solide Sicherheitsinitiative umfasst mehrere Ebenen und wird ständig weiterentwickelt. Es ist zwecklos, die Haustür abzuschließen, wenn sich Einbrecher über ein geöffnetes Fenster Zugang verschaffen können. Einer Studie zufolge bieten herkömmliche Maßnahmen wie Firewalls und Antivirenprogramme in den meisten Fällen keinen Schutz vor Hackern, während Endgeräte-Sicherheitstechnologien Angriffe effektiver abwehren können.[4]

„Wir hatten noch keine Datenpanne, also funktioniert unsere Sicherheit gut."

Vielleicht wissen Sie gar nicht, dass es bereits zu einer Sicherheitsverletzung gekommen ist. Studien zufolge kann es 197 Tage dauern, bis Unternehmen eine Datenpanne entdecken.[3]

„Wir haben bereits ein formales Sicherheitsprogramm."

Gut! Wird es kontinuierlich weiterentwickelt, um mit den sich ständig ändernden Bedrohungen Schritt zu halten? Deckt es Ihre gesamte Technologie ab? Um den raffinierten Cyberkriminellen von heute gewachsen zu sein, ist ein umfassender Ansatz nötig.

„Sicherheit ist zu kompliziert."

Durchdachte Sicherheitsmaßnahmen sind intuitiv und einfach zu implementieren. Sie schützen Ihre Mitarbeiter nahtlos und können von Ihrer IT-Abteilung einfach verwaltet werden.

„Sicherheit beeinträchtigt die Produktivität."

Häufig wird geklagt, dass Sicherheitssysteme zu umständlich und schwer zu integrieren sind, oder dass sie die Abläufe verlangsamen. Eine Datenpanne kann Ihren Betrieb jedoch vollständig lahmlegen. Die Lösung besteht darin, Technologie mit integrierter Sicherheit zu wählen. Dann kann Sicherheit die Produktivität sogar erhöhen.

Sichern Sie Ihr Unternehmen durch mehrere Schutzebenen

Nicht alle Sicherheitsmaßnahmen werden Ihren Anforderungen gerecht. Berücksichtigen Sie bei der Auswahl von Technologie die folgenden wichtigen Sicherheitsattribute, die Zebra Technologies Ihnen bietet.

Integrierte Sicherheit und Performance:
Entscheiden Sie sich für den Hersteller, der Sicherheit und Produktivität von Anfang an in die Technologie integriert. Sie werden feststellen, dass unsere Lösungen speziell entwickelt wurden, um Ihre Leistung zu steigern. Gleichzeitig wurde eine Reihe von äußerst effektiven Sicherheitsprotokollen und -funktionen integriert.

Automatisierte Sicherheitsfunktionen:
Wi-Fi®-Zertifizierungen, mit denen Ihre IT-Abteilung früher mehrere Wochen beschäftigt war, können jetzt automatisch durchgeführt werden. So stehen Sicherheitsfunktionen in vernetzten Umgebungen Ihnen und Ihrem Team schneller zur Verfügung.

An Ihre Anforderungen anpassbar:
Möchten Sie Ihre Sicherheitstoleranz lieber selbst festlegen? Zebra macht es Ihnen leicht mit konfigurierbaren Lösungen, die eine einfache Anpassung des Sicherheitsniveaus an die Bedürfnisse Ihres Unternehmens oder Ihrer Abteilung ermöglichen.

Unkomplizierte Wartung und einfacher Support:
Unsere Sicherheitsfunktionen, Software und Hardware benötigen minimale Wartung bei maximalen Betriebszeiten – darauf haben wir bei der Entwicklung und beim Testen geachtet. Zudem steht Ihnen unser Supportteam bei Bedarf rund um die Uhr zur Verfügung.

Mühelose Integration:
Zebra bietet eine reibungslose, schnelle Integration. Da wir umfassend mit Ihrer Branche und Ihren Anwendungen vertraut sind, sind unsere Lösungen so konzipiert, dass sie Ihre Integrationsanforderungen antizipieren und erfüllen.

Kontinuierliche Überwachung und Support:
Sie erhalten über Jahre hinweg OS-Sicherheitsupdates und Firmware-Verbesserungen und profitieren von Fehlerbehebung, Schwachstellenanalysen sowie interner Zusammenarbeit bei der Sicherheit.

Einhaltung weltweit anerkannter Best Practices:
Zebra hält Best Practices und Richtlinien ein, die von globalen Sicherheitsexperten festgelegt wurden, darunter die Internationale Organisation für Normung (ISO), das National Institute of Standards and Technology (NIST) und das Center for Internet Security Benchmark Controls. Unsere Produkte und Lösungen werden in Anwendungen eingesetzt, die Unternehmen bei der Einhaltung der Vorgaben des HIPAA, PCI-DSS und der DSGVO unterstützen.

Führend bei sicherer Enterprise-Technologie:
Vertrauen Sie dem Hersteller, der die Sicherheit des Google-Betriebssystems Android™ für den Einsatz in Unternehmensumgebungen erhöht hat und bis zu zehn Jahre OS-Sicherheitssupport bietet. Von unseren robusten mobilen Computern der Enterprise-Klasse über unsere sicheren Drucker bis hin zu unseren visionären Technologien – Produktivität und Sicherheit stehen im Mittelpunkt unseres Handelns.

Produkte, Lösungen und Dienstleistungen von Zebra Unterstützung aller Phasen des NIST Cybersecurity Framework

IDENTIFIZIEREN	Risikomanagement und -überwachung Assistent zur Bewertung der Druckersicherheit Professional Services	Lieferketten-Risikomanagement Sicherheitsausschuss
SCHÜTZEN	LifeGuard™ für Android „Protected Mode“ für Drucker Gerätesteuerung	PrintSecure-Updates Automatisierter WLAN-Zertifikatmanager Risikomanagement-Richtlinien
ERKENNEN	Printer Profile Manager Enterprise Sicherheitsüberwachung	Erkennung in Echtzeit
REAGIEREN	Geräteverwaltung Maßnahmen zur Bedrohungserkennung	Reaktion auf Vorfälle Benachrichtigung von Kunden
WIEDERHERSTELLEN	Professional Services Verbesserungen	Wiederherstellung auf bekannten Zustand

Schützen Sie Ihren Leistungsvorteil

Sicherheit ist für Ihr Unternehmen und Ihre Arbeitsabläufe von entscheidender Bedeutung. Zebra schützt durch die Integration mehrerer Sicherheitsebenen in seine Lösungen proaktiv vor Schwachstellen. Geräte, Technologie und Dienstleistungen von Zebra sind auf Sicherheit ausgelegt, ohne die Produktivität zu beeinträchtigen. Unsere Sicherheit lässt sich einfach bereitstellen und schützt Ihre Mitarbeiter im direkten Kundenkontakt nahtlos. Mit unserer intelligenten, konfigurierbaren Technologie können Sie betriebliche Ziele und Sicherheit in der Praxis in Echtzeit in Einklang bringen. Zebra bietet Ihnen die Sicherheit, die Sie für die Umsetzung Ihrer Geschäfts- und Technologiestrategien am Netzwerkrand benötigen.

ZEBRA

Erfahren Sie, wie unsere Sicherheitsstandards Ihre Sicherheit verbessern.
Gehen Sie zu **www.zebra.com/product-security.**

Quellen:
1. Juniper Research, 2018 **2.** Carbon Black Incident Response Threat Report, Nov. 2018 **3.** Ponemon Institute, 2018 and 2019 Cost of Data Breach **4.** Black Report, Nuix 2017 **5.** Shape Credential Spill Report 2018 **6.** Verizon 2019 Data Breach Investigations Report