Software-Sicherheit in der gesamten Intelligent Edge

Sicherheit muss jedes einzelne Endgerät im gesamten Lebenszyklus umfassen

WNDRVR

Die Sicherheit wird von drei Dynamiken beeinflusst

Bis 2025 werden sich zwei Milliarden PCs und 42 Milliarden vernetzte Geräte für das Internet of Things in unserer Welt etabliert haben.

Nahezu jedes Gerät wird in irgendeiner Weise mit der Cloud arbeiten, und 80% der Daten, die wir alle erstellen, mit denen wir umgehen und intensiv arbeiten, werden die 5G-Cloud durchlaufen. Derzeit sind jedoch nur 11,5% aller Unternehmen dabei, den digitalen Wandel erfolgreich zu bewältigen.[1] Das bedeutet, dass die meisten Unternehmen noch vor großen Herausforderungen stehen, um in der kommenden digital bestimmten Welt mithalten zu können.

Unter diesen Herausforderungen steht die Sicherheit ganz oben. Denken Sie nur daran, wie komplex das Design von Sicherheitsprotokollen in dieser neuen Welt ist, die sich gerade entwickelt. Mehr als die Hälfte der Technologieführer sehen verschiedene Sicherheitsbedenken in direktem Zusammenhang mit den Initiativen zur digitalen Transformation, einschließlich erhöhter Cybersicherheitsrisiken (53%), cyberkrimineller Komplexität (56%) und erhöhter Angriffsfläche (53%). Zu diesen Bedrohungen gesellt sich eine weitere Sorge, die von 40% der CISOs, CTOs und CIOs geteilt wird: nämlich die Probleme, die durch eine starre technologische Infrastruktur verursacht werden – die Art von Infrastruktur, die eng mit Embedded-Systemen verbunden ist.[2]

40%

der CISOs, CTOs und CIOs sind besorgt über die Probleme, die durch eine starre technologische Infrastruktur verursacht werden – die Art von Infrastruktur, die eng mit Embedded-Systemen verbunden ist.

Bedenken Sie drei Dynamiken, die sich ständig um uns herum verändern und die auf den folgenden Seiten näher erläutert werden.

1 *Forbes/Inc.Digital*
2 *media.nominet.uk/wp-content/uploads/2019/07/Cyber-Security-in-the-Age-of-Digital-Transformation.pdf*

EMERSON
Network Power

WIE HAT EMERSON SEIN OVATION DCS BESSER VERNETZT UND SICHERER GEMACHT?

Mit Machine Learning, Simulation des kompletten Systems und Wind River.

Die DCS-Plattform (Distributed Control System) Ovation™ entwickelt sich mit der sich ändernden Technologie weiter, um die Zuverlässigkeit von Kraftwerken zu erhöhen, und wurde vom Department of Homeland Security (DHS) im Rahmen des U.S. SAFETY Act als qualifizierte Antiterrorismus-Technologie eingestuft.

Emerson setzt Wind River®-Lösungen für den gesamten Lebenszyklus von Ovation ein: Beschleunigung der Entwicklung mit virtueller Hardware, VxWorks® als zugrunde liegendes Betriebssystem für das DCS, Simulation der gesamten physikalischen Umgebung der Anlage und – entscheidend für die Betriebssicherheit – Modellierung des Steuerungssystembetriebs. Diese Lebenszykluslösungen bieten eine Ausgangsbasis für Systemparameter und -leistung, mit deren Hilfe ungewöhnliche Verhaltensweisen erkannt werden können, bevor sie sich auf Produktionssysteme auswirken.

Dynamik 1

DER WERT DER DATEN IST DYNAMISCHER GEWORDEN ALS DIE 0,1% IHRES LEBENSZYKLUS, FÜR DIE SIE KONZIPIERT WURDEN UND IN DER SIE EINE ROLLE SPIELEN.

Einen Kernfokus auf ein Gerät zu legen, wird kaum dem Trend der Zukunft entsprechen. Der Wert von Daten ist in einer digital zentrierten Welt viel dynamischer. Die Tatsache, dass 75 % der Führungskräfte von Großunternehmen angeben, dass sie 200 % weniger Zeit als früher haben, um Entscheidungen zu treffen,[3] verdeutlicht die Notwendigkeit, dass Daten schnell zur Verfügung stehen müssen, um die Entscheidungsfindung zu unterstützen.

Daten sind mehr denn je dynamischer Natur, zum Teil deshalb, weil sie von Tausenden oder Millionen von verschiedenen Orten stammen und oft zur gleichen Zeit eintreffen. Wofür diese Daten verwendet werden können, hängt von den entscheidenden Momenten ab.[4] Dieser Moment spielt möglicherweise nur in 0,1 % der Lebensdauer des Geräts eine Rolle – wenn wir es nur auf der Grundlage des ursprünglichen Designs bauen. In einer dynamischen Welt könnte der Wert der Daten, die in den anderen 99,9 % der Lebensdauer des Geräts gesammelt werden, für andere Teile der Dateninfrastruktur wertvoll sein. In einer vernetzten Welt haben Daten einen vielschichtigen Wert, der oft weit über das Kerndesign des Geräts hinausgeht.

Die Bedeutung der Datenrevolution, die bei den Geräten im Gange ist, wird durch den Kampf um den Schutz dieser Daten unterstrichen. Mehr als die Hälfte aller IoT-Geräte ist anfällig für Angriffe mit mittlerem oder hohem Schweregrad. Und 98 % des gesamten Datenverkehrs mit IoT-Geräten – einschließlich des Datenverkehrs mit medizinischen Geräten – bleibt unverschlüsselt.[5] Bestimmte Datenklassen erfordern fein ausdifferenzierte Überlegungen zu den Auswirkungen auf den Datenschutz, da die dynamische Natur der Daten bedeutet, dass es sich um Personenbezogene Identifizierbare Informationen (PII) handeln könnte, die weltweit unterschiedlichen Vorschriften unterliegen.[6]

> Stellen Sie sich vor, dass Daten einen Netzwerkeffekt haben: Je mehr Geräte sich in Echtzeit verbinden, desto größer ist der Wert der Informationen und Daten für das Unternehmen.

98%

des gesamten Datenverkehrs mit IoT-Geräten – einschließlich des Datenverkehrs mit medizinischen Geräten – bleibt unverschlüsselt.

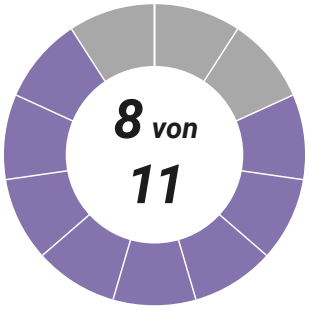
3 *Forbes/Inc.Digital*
4 *The Digital Helix*
5 *threatpost.com/half-iot-devices-vulnerable-severe-attacks/153609*
6 *www.varonis.com/blog/data-privacy*

Dynamik 2

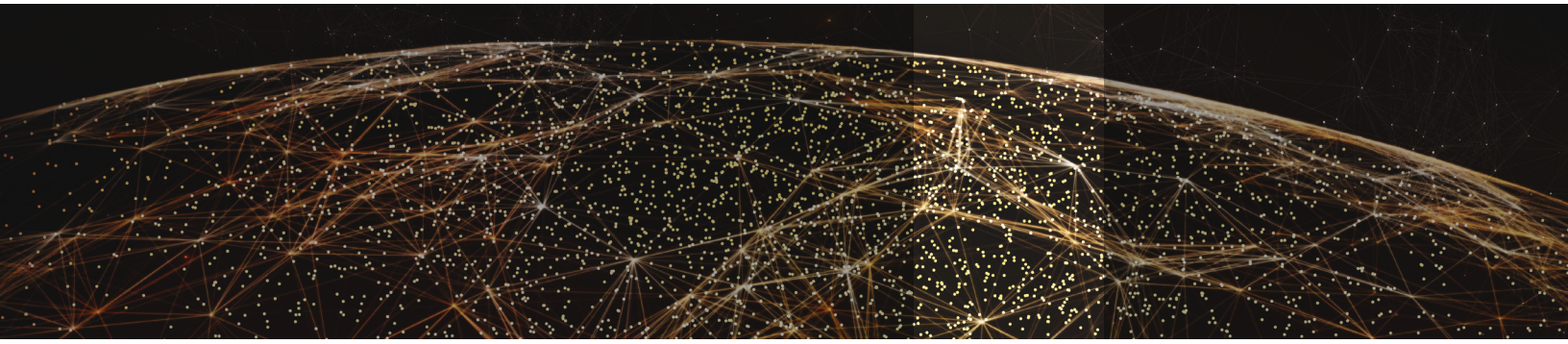
SICHERHEIT MUSS PARTNERSCHAFTSÜBERGREIFEND FUNKTIONIEREN (INNERHALB UND AUSSERHALB VON ORGANISATIONEN)

Stellen Sie sich vor, Sie haben eine Komponente in einer Industriemaschine, die den komplexen Stromaustausch über ein komplettes Stromnetz verwaltet. Dieses Gerät könnte auch in den Produkten von zehn anderen Ökosystempartnern enthalten sein, die alle zusammenarbeiten. Sie möchten wissen, welche Leistung diese Komponente erbringt und auch, wie das gesamte Daten-Ökosystem wertschöpfende Erkenntnisse liefert, die in Echtzeit genutzt werden können. Vielleicht möchten Sie sehen, wie diese Daten in Zukunft auf verschiedene Weise arrangiert werden könnten. Solche Gelegenheiten für aufschlussreiche Erkenntnisse gibt es in den Bereichen Energieverteilung, Herstellung medizinischer Geräte, Luftfahrt und Verteidigung sowie in anderen Sektoren, in denen die Leistung des Geräts über seine Kernfunktionalität hinausgeht.

Stellen Sie sich vor, dass Daten einen Netzwerkeffekt haben: Je mehr Geräte sich in Echtzeit verbinden, desto größer ist der Wert der Informationen und Daten für das Unternehmen. Angesichts der von Forbes/Inc.Digital untersuchten digitalen Transformationsstrategien waren 8 von 11 Branchenführern davon überzeugt, dass Einfluss und Macht von Daten in einer sich digital wandelnden Welt ihren zukünftigen Erfolg mitbestimmen werden. Und je mehr Partner im Ökosystem beteiligt sind, desto größer ist die potenzielle Macht der Daten. Dieses Argument mag abstrakt klingen, aber jüngste Arbeiten der IBM-Gruppe Cognitive Systems zeigen, dass die beste und wirtschaftlich effektivste KI dadurch entsteht, dass alle vier KI-Formate (Machine Learning, Deep Learning, visuelle Erfassung und natürliche Sprache) gleichzeitig ausgeführt werden: mehrere Datensätze, die in Echtzeit zusammenarbeiten. Da KI fast alles durchdringt, ist die Macht von Datenpartnerschaften enorm wichtig und liefert weit mehr Wert, als nur ein einziges Ökosystem bieten kann.



8 von 11 Branchenführern waren überzeugt, dass Einfluss und Macht von Daten in einer sich digital wandelnden Welt ihren zukünftigen Erfolg mitbestimmen werden.



Dynamik 3

DIE NEUE DIGITALE ZUKUNFT IST NICHT KLAR VORHERBESTIMMBAR. KANN IHR SICHERHEITSDESIGN MIT DIESER UNKARHEIT UMGEHEN?

Ambiguität ist unsere neue digitale Zukunft. Transformation generell ist eine schwierige Angelegenheit. Daher sind auch die Transformation unseres Sicherheitsdesigns und die entsprechende Durchführung keine einfache Sache. Allerdings blicken Großunternehmen (Fortune-Global-2000-Unternehmen), die mit ihrer digitalen Transformation sehr gut vorankommen, exponentiell zuversichtlicher in die Zukunft, weil sie Umgebungen zum Umgang mit dieser Ambiguität schaffen.

Unsere volatile, unsichere, komplexe und mehrdeutige Welt (VUCA, volatile, uncertain, complex, ambiguous) verlangt von uns, dass wir über neue Wege der Sicherheit nachdenken. Die Fähigkeit, sich mit dieser Realität eingehend zu befassen, ist von wesentlicher Bedeutung, da die Geschwindigkeit der effektiven digitalen Transformation (CAGR, Compound Annual Growth Rate, jährliche Wachstumsrate) langsam war: 11,5 % seit 2013.[7] Worauf wir uns einstellen müssen, ist eine Zukunft, in der wir in der Lage sind, Daten zu schützen und zu ermöglichen, dass die Erkenntnisse aus diesen Daten in Echtzeit genutzt und letztlich über mehrere Ökosysteme hinweg ausgetauscht werden können.

In der prädigitalen Welt herrschte ein gutes Verständnis davon, was Sicherheit bedeutet. Nun müssen sich die Konstrukte, die für den Einbau von Sicherheit benötigt werden, täglich neu anpassen, genau wie KI, die Cloud und 5G. Eine Zukunft mit intelligenten Edge-Geräten, die für eine anpassungsfähige Welt konzipiert sind, muss das vorrangige Ziel für Entwickler und Anwendungsmanagement sein.

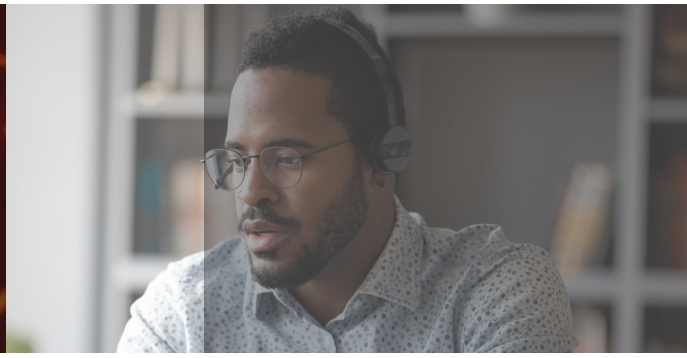
Beantworten Sie eingehend drei einfache Fragen, um zu sehen, wie gut Sie für diese neue digitale Welt aufgestellt sind:

1. Arbeiten Sie zunehmend mit neuen Design-Sicherheitsanforderungen für Ihre Geräte?
2. Wird die VUCA-Welt, in der wir leben, von der Organisation als Bereicherung betrachtet, oder werden Sie durch Sicherheitserfordernisse gebremst bzw. in einer guten Entwicklung beschleunigt?
3. Ist es wahrscheinlich, dass sich Ihre grundlegende Sicherheitsstrategie in fünf Jahren, in denen Sie sich als Organisation digital wandeln, stark verändern wird?

> "Indem wir ein Simulationsmodell (VxWorks Simulator) parallel zu seiner entsprechenden Embedded-Hardware verwenden, können wir es zum goldenen Standard machen und potenziell in der Lage sein, ungewöhnliches Verhalten zu erkennen, bevor es sich tatsächlich als Systemausfall manifestiert."
>
> **—Rick Kephart,**
> *Vice President, Software Development, Emerson*

7 *Inc.Digital*

Die Edge



Wir erschaffen und schützen die neue digitale Realität im Verlauf von zwei umfassenden Veränderungen: einem massiven Übergang zu Edge-Computing, insbesondere in der Art und Weise, wie Unternehmensdaten erfasst, verarbeitet und gespeichert werden; und einem Generationswechsel unter den Beschäftigten, die die geschäftskritischen, intelligenten, vernetzten Systeme der Zukunft entwickeln und betreiben werden.

Im Jahr 2018 wurden nur 10 % der Unternehmensdaten außerhalb eines herkömmlichen Rechenzentrums erfasst und verarbeitet; bis 2025 wird dieser Prozentsatz auf mehr als 75 % anwachsen.[8] In der Zwischenzeit, im Jahr 2020, wurden die Millennials zum größten Prozentsatz der Beschäftigten.[9]

ERFAHRUNG IST WICHTIG

Die Generation von Entwicklern und Bedienern mit der größten Erfahrung mit älteren Embedded-Systemen nähert sich dem Rentenalter, während ein viel kleinerer Pool von talentierten Embedded-Engineering-Spezialisten in den Startlöchern steht. 82 % der Führungskräfte berichteten über einen Mangel an qualifizierten Bewerbern im technischen Bereich, wobei 60 % der Unternehmen angaben, dass Arbeitsplätze in der Elektrotechnik am schwierigsten zu besetzen sind.[10] Erfahrung mit IoT-Systemen ist entscheidend, um diese jederzeit zu schützen, da Programmierfehler eine der Hauptursachen für Schwachstellen in der CVE-Datenbank (Common Vulnerabilities and Exposures) sind: „Die meisten Angriffe richten sich gegen Betriebssysteme und Firmware: Programmierfehler in dieser Software und schwache Zugriffskontrolle oder schwache Authentifizierung ermöglichen Angriffe auf der untersten softwarebasierten Ebene, aber die nicht offengelegten Schwachstellen betreffen häufig auch diese Software."[11]

8 *www.gartner.com/smarterwithgartner/what-edge-computing-means-for-infrastructure-and-operations-leaders*
9 *Forbes/Inc.Digital*
10 *www.semi.org/en/node/581*
11 *www.cse.psu.edu/~pdm12/cse5979-f15/readings/cse5979-embedded_systems.pdf*

TOSHIBA

WIE SCHÜTZT TOSHIBA PERSONENBEZOGENE DATEN IN EINEM MARKT, IN DEM CYBERKRIMINALITÄT UNTERNEHMEN IN DEN NÄCHSTEN FÜNF JAHREN 5,2 BILLIONEN DOLLAR KOSTEN WIRD?

60 % der unerlaubten Zugriffe im Jahr 2019 betrafen Schwachstellen, für die zwar ein Patch verfügbar aber nicht angewendet war. Wind River Linux hilft Toshiba, diese Quoten zu verändern.

Im Jahr 2019 wurden mehr als 45 CVEs, also Sicherheitsschwachstellen, pro Tag protokolliert. Das Elektronik- und IT-Konglomerat Toshiba hat die Risiken erkannt, die CVEs für die in seinem Besitz befindlichen personenbezogenen Daten darstellen, und geht daher eine Partnerschaft mit Wind River ein, um seine Daten zu schützen und Kosten zu senken. Das Wind River-Sicherheitsteam überwacht die CVE-Datenbank durchgängig auf potenzielle Probleme, die VxWorks und alle Funktionen des Wind River Linux-Kernel, Benutzerpakete und Tools betreffen. Darüber hinaus überwacht das Team Benachrichtigungen von US-Regierungsbehörden und-organisationen wie NIST und US-CERT sowie Mailinglisten von öffentlichen und privaten Sicherheitsdiensten auf Warnmeldungen.

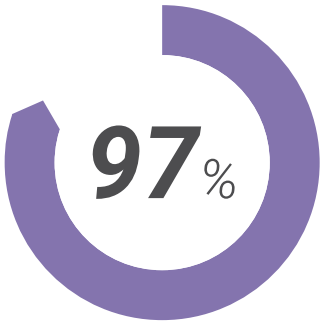
ZUGANG IST ALLES

IoT- und andere Edge-Geräte sind oft physisch zugänglich und einer Reihe von hardwarebasierten Angriffen ausgesetzt, die in besser kontrollierten Umgebungen kaum auftreten. Die Risiken werden noch dadurch erhöht, dass solche Systeme auch nach dem Kauf auf dem Markt erhältlich sind (Aftermarket), so dass Cyberkriminelle in aller Ruhe Angriffe entwickeln können. Geräte, die klein sind, sich in Privatbesitz befinden und nicht unter dem Gesichtspunkt der Sicherheit gebaut wurden, werden eventuell nicht regelmäßig aktualisiert und können einen einfachen Zugang zu dem umfassenderen Netzwerk bieten, mit dem sie verbunden sind. In einer Umfrage des Ponemon Institute aus dem Jahr 2018 äußerten 97 % der Risikomanagement-Experten die Auffassung, dass ungesicherte IoT-Geräte für einen „katastrophalen" Sicherheitsverstoß anfällig sein könnten.[12]

Drei Fragen, die Sie stellen müssen, wenn Sie sich der Edge annähern:

1. Haben Sie Zugang zu talentierten Ingenieuren mit den vielfältigen Fähigkeiten, die für die Entwicklung, Implementierung und Wartung der heutigen IoT-Geräte und verwandter Systeme erforderlich sind?
2. Verfügen Sie über eine Strategie zur digitalen Erfahrung, die sicherstellt, dass Ihre Geräte von einer Mehrheit der Millennials und Digital Natives in Ihrer Belegschaft problemlos bedient werden können?
3. Verstehen Sie die Lieferkette lückenlos, in die Ihr Gerät passt – einschließlich Ihrer Software-Lieferkette unter Berücksichtigung der Aftermarket-Lieferanten?

> "Es gibt Aktualisierungen, die jeden Tag für potenzielle Sicherheitsrisiken verfügbar sind. Wir haben hier beim TGCS ein Team, das sich genau darauf konzentriert. In Zusammenarbeit mit Wind River stellen wir sicher, dass die bekannten Risiken erkannt werden und dass wir für unsere Händler schnell reagieren."
>
> **—Gregg Margosian,**
> *COO, Toshiba*



97% der Risikomanagement-Experten sind der Auffassung, dass ungesicherte IoT-Geräte für einen „katastrophalen" Sicherheitsverstoß anfällig sein könnten.

12 *sharedassessments.org/wp-content/uploads/2018/04/2018-IoTThirdPartyRiskReport-Final-04APR18.pdf*

Definition einer Sicherheitsrichtlinie

49% der Design-Teams betrachten die Definition einer Sicherheitsrichtlinie als eines ihrer wichtigsten Projekte.

Die CIA-TRIAD stellt ein Modell nach Industriestandard dar, das zur Entwicklung einer Sicherheitsrichtlinie anleitet und die notwendigen Prinzipien definiert, um ein Gerät vor unbefugtem Zugriff, unbefugter Nutzung, Offenlegung, Unterbrechung, Änderung oder Zerstörung zu schützen.

CIA steht für Confidentiality (Vertraulichkeit), Integrity (Integrität), Availability (Verfügbarkeit):

- **Vertraulichkeit** simplementierungen werden verwendet, um die Vertraulichkeit von Daten in IoT-Systemen zu schützen. Dazu gehören Daten, die gerade übertragen werden, Daten, die sich in Ruhe befinden oder auf dem Gerät gespeichert sind, Daten, die vom Gerät verarbeitet werden, sowie Daten, die zu und von dem Gerät übertragen werden.
- **Integrität** simplementierungen stellen sicher, dass die Gerätedaten nicht von einem Angreifer verändert oder gelöscht wurden. Dazu gehören sowohl Daten, die vom Embedded-Gerät erzeugt oder verwendet werden, als auch seine Programmierdaten (Betriebssystem, Anwendungen, Konfigurationsdaten usw.).
- **Verfügbarkeit** simplementierungen werden verwendet, um sicherzustellen, dass ein IoT-Gerät seine vorgesehene Funktion erfüllt. Das bedeutet, dass ein Angreifer den beabsichtigten Funktionszweck eines Geräts nicht ändern kann. Dies ist von größter Bedeutung für Geräte, die lebenswichtige oder geschäftskritische Aufgaben erfüllen.

Projektteams legen fest, welche Komponenten der CIA-TRIAD erforderlich sind, und zwar auf der Grundlage von Risikoexposition, behördlichen Anforderungen und des IP-Schutzbedarfs im Verhältnis zu den Kosten, der Leistung und der Betriebsumgebung des implementierten Geräts. Es gibt keine Patentlösung, um ein Gerät oder System vor allen möglichen Angriffen zu schützen. Vielmehr bietet ein mehrschichtiger Ansatz, der verschiedene Kontrollmechanismen zur Risikominderung einsetzt, ein facettenreiches Schutzschild und letztlich eine viel stärkere Umsetzung der Cybersicherheit.

Es gibt keine Patentlösung, um ein Gerät oder System vor allen möglichen Angriffen zu schützen. Vielmehr bietet ein mehrschichtiger Ansatz, der verschiedene Kontrollmechanismen zur Risikominderung einsetzt, ein facettenreiches Schutzschild und letztlich eine viel stärkere Umsetzung der Cybersicherheit.

Fragen, die Sie stellen müssen, wenn Sie sich der Edge annähern

GELINGT IHNEN DIE TRANSFORMATION ODER ERWEITERN SIE UNBEWUSST DIE ANGRIFFSFLÄCHE?

Fünf Sicherheitsfragen, die beim digitalen Wandel zu beantworten sind

Mit der zunehmenden Digitalisierung der Welt der Embedded-Systeme und der OT-Domäne (Operational Technology) und der Tatsache, dass sich der Lebenszyklus von Geräten über Geräte mit festen Funktionen und Geräte, die beschädigt und repariert werden, hinaus bewegt, werden grundlegend andere Strategien erforderlich sein, um die nächste Generation kritischer Systeme sicher zu designen, zu implementieren, zu arrangieren und anzupassen.

1. Konzentriert sich Ihre Sicherheitsstrategie in erster Linie auf die Endpunkte, oder handelt es sich wirklich um einen Ansatz auf Systemebene, der die Cloud umfasst und eine Chain of Custody für die Daten im Zentrum des digitalen Wandels bietet?
2. Verfügen Sie über eine etablierte Methodik für die gleichzeitige Entwicklung der Funktionalität und der Sicherheitselemente Ihrer IoT-Systeme, und wenn ja, unterstützt diese Methodik die Verbreitung von Bedrohungen, die mit dem digitalen Wandel einhergehen?
3. Unterstützt Ihre Systemarchitektur die effiziente Verwaltung und Aktualisierung von Edge-Geräten von der Implementierung an, wobei die nächste Generation von Sicherheitsbedrohungen antizipiert wird und die erforderliche Flexibilität möglich ist, um die Sicherheit über Jahrzehnte vor Ort sicherzustellen?
4. Erkennen Ihre vorhandenen Unternehmenssicherheitstools die verschiedenen branchenspezifischen Protokolle Ihrer IoT-Systeme, und wenn nicht, wie werden Sie das Eindringen über diese Protokolle erkennen, wo der digitale Wandel die Konvergenz von Unternehmen und Edge beschleunigt?
5. Umfasst der Sicherheitsbereich Ihres Unternehmens auch Geräte, die vor Ort implementiert sind, und wenn nicht, wie werden Sie eine sichere Verbindung zwischen diesen Geräten und dem Unternehmen sicherstellen?

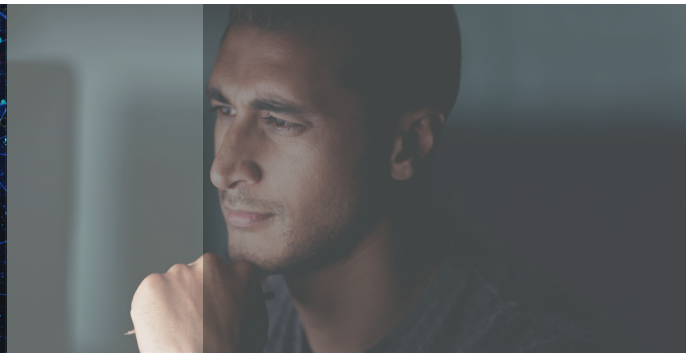
SENDEN SIE DATEN IM KLARTEXT?

Drei Sicherheitsfragen, die beim Bau und der Implementierung datenzentrischer Geräte beantwortet werden müssen

Gerätehersteller müssen sich das neue digitale Paradigma der Interkonnektivität und Datendynamik zu eigen machen und Sicherheit konzipieren: nicht nur für Daten im Speicher, sondern auch für Daten, die ein System bzw. Netzwerk durchlaufen, und für die Schlüssel, die zur Verschlüsselung dieser Daten verwendet werden. In der Zwischenzeit müssen sie auch sicherstellen, dass Software und Hardware gegen Manipulationen, die die Datenintegrität beeinträchtigen, widerstandsfähig sind. Verfügt Ihre Organisation über einen umfassenden Ansatz für Datensicherheit und Datenschutz, oder konzentrieren sich Ihre Entwicklungsbemühungen ausschließlich auf die Sicherheit der Endpunkte?

1. Werden die von Ihnen entwickelten Systeme zu den 98% der IoT-Geräte gehören, die Daten im Klartext senden, oder werden Sie Ihre Daten verschlüsseln?
2. Haben Sie ein klares Verständnis der Implementierungsumgebung, in der Ihre Systeme eingesetzt werden sollen, der Angriffe, denen diese Umgebung ausgesetzt sein kann, und der Art und Weise, wie Überlegungen zum Datenschutz Eingang in die Implementierungsumgebung finden können oder nicht?
3. Haben Sie eine Teststrategie, um das gesamte Spektrum der Bedrohungen für die Datensicherheit anzugehen?

Was spricht für Wind River?



Seit fast 40 Jahren unterstützt Wind River die weltweit führenden Technologieunternehmen dabei, die sichersten Geräte der Welt zu erschaffen, und das Generation für Generation.

Und in einer neuen Ära der Autonomie und Konnektivität ist Wind River weiterhin führend. Unsere Software betreibt die Computersysteme der wichtigsten modernen Infrastruktur, die nicht ausfallen dürfen, einschließlich Flugzeuge, Eisenbahnen, Autos, medizinischer Geräte, Fertigungsanlagen und Kommunikationsnetzwerke.

Unsere Technologie ist in mehr als 2 Milliarden Geräten auf der ganzen Welt enthalten und wird durch unsere branchenführenden Professional Services, unseren angesehenen Customer Service und unser breitgefächertes Partner-Ökosystem unterstützt.

Unsere Kunden können hochmoderne, robuste und zuverlässige Software-Plattformen nutzen, die Privacy schützen, Datenintegrität jederzeit gewährleisten und Verfügbarkeit durch nahtlose Systemintegration und Zusammenarbeit zwischen Entwicklern sicherstellen.

> Unsere Plattformen dienen als vertrauenswürdige Grundlage, damit Sie sicher innovativ arbeiten und Ihr Gerät vor aktuellen und zukünftigen Bedrohungen schützen können.

Wind River is a global leader of software for the intelligent edge. Its technology has been powering the safest, most secure devices since 1981 and is in billions of products. Wind River is accelerating the digital transformation of mission-critical intelligent systems that demand the highest levels of security, safety, and reliability.

© 2021 Wind River Systems, Inc. The Wind River logo is a trademark of Wind River Systems, Inc., and Wind River and VxWorks are registered trademarks of Wind River Systems, Inc. Rev. 01/2021

Anhang

Arbeitsblatt Sicherheit für die neue digitale Welt

STELLEN SIE SICH FÜR EINE NEUE DIGITALE, UNBESTÄNDIGE, UNSICHERE, KOMPLEXE UND MEHRDEUTIGE (VUCA-) WELT ENTSPRECHEND AUF?

1. Arbeiten Sie zunehmend mit neuen Design-Sicherheitsanforderungen für Ihre Geräte?
2. Wird die VUCA-Welt, in der wir leben, von der Organisation als Bereicherung betrachtet? Werden Sie durch Sicherheitserfordernisse gebremst oder in einer guten Entwicklung beschleunigt?
3. Ist es wahrscheinlich, dass sich Ihre grundlegende Sicherheitsstrategie in fünf Jahren, in denen Sie sich als Organisation digital wandeln, stark verändern wird?

GELINGT IHNEN DIE TRANSFORMATION ODER ERWEITERN SIE UNBEWUSST DIE ANGRIFFSFLÄCHE?

1. Konzentriert sich Ihre Sicherheitsstrategie in erster Linie auf die Endpunkte, oder handelt es sich wirklich um einen Ansatz auf Systemebene, der die Cloud umfasst und eine Chain of Custody für die Daten im Zentrum des digitalen Wandels bietet?
2. Verfügen Sie über eine etablierte Methodik für die gleichzeitige Entwicklung der Funktionalität und der Sicherheitselemente Ihrer IoT-Systeme, und wenn ja, unterstützt diese Methodik die Verbreitung von Bedrohungen, die mit dem digitalen Wandel einhergehen?
3. Unterstützt Ihre Systemarchitektur die effiziente Verwaltung und Aktualisierung von Edge-Geräten von der Implementierung an, wobei die nächste Generation von Sicherheitsbedrohungen antizipiert wird und die erforderliche Flexibilität möglich ist, um die Sicherheit über Jahrzehnte vor Ort sicherzustellen?
4. Erkennen Ihre vorhandenen Unternehmenssicherheitstools die verschiedenen branchenspezifischen Protokolle Ihrer IoT-Systeme, und wenn nicht, wie werden Sie das Eindringen über diese Protokolle erkennen, wo der digitale Wandel die Konvergenz von Unternehmen und Edge beschleunigt?
5. Umfasst der Sicherheitsbereich Ihres Unternehmens auch Geräte, die vor Ort implementiert sind, und wenn nicht, wie werden Sie eine sichere Verbindung zwischen diesen Geräten und dem Unternehmen sicherstellen?

SENDEN SIE DATEN IM KLARTEXT?

1. Werden die von Ihnen entwickelten Systeme zu den 9 % der IoT-Geräte gehören, die Daten im Klartext senden, oder werden Sie Ihre Daten verschlüsseln?
2. Haben Sie ein klares Verständnis der Implementierungsumgebung, in der Ihre Systeme eingesetzt werden sollen, der Angriffe, denen diese Umgebung ausgesetzt sein kann, und der Art und Weise, wie Überlegungen zum Datenschutz Eingang in die Implementierungsumgebung finden können oder nicht?
3. Haben Sie eine Teststrategie, um das gesamte Spektrum der Bedrohungen für die Datensicherheit anzugehen?

VERFÜGEN SIE ÜBER DAS NÖTIGE WISSEN FÜR DEN ERFOLG, WÄHREND SIE SICH DER EDGE ANNÄHERN?

1. Haben Sie Zugang zu talentierten Ingenieuren mit den vielfältigen Fähigkeiten, die für die Entwicklung, Implementierung und Wartung der heutigen IoT-Geräte und verwandter Systeme erforderlich sind?
2. Verfügen Sie über eine Strategie zur digitalen Erfahrung, die sicherstellt, dass Ihre Geräte von einer Mehrheit der Millennials und Digital Natives in Ihrer Belegschaft problemlos bedient werden können?
3. Verstehen Sie die Lieferkette lückenlos, in die Ihr Gerät passt – einschließlich Ihrer Software-Lieferkette unter Berücksichtigung der Aftermarket-Lieferanten?