WHITE PAPER

Sinteso EN Produktfamilie:
Cybersecurity trifft Brandschutzsysteme

siemens.de/brandschutz

SIEMENS

Executive Overview

Für den Schutz Ihrer Mitarbeiter, Ihrer Vermögenswerte und Ihres Unternehmens ist es von entscheidender Bedeutung, dass Ihre Brandschutzsysteme stets auf dem neuesten Stand sind. Sie investieren Zeit und Mühe in ein gut durchdachtes System, das gewährleistet, dass die richtigen Elemente vorhanden sind - von der Erkennung, Alarmierung, Evakuierung und Löschung bis hin zum Gefahren- und Gebäudemanagement. Und Sie stellen sicher, dass die Brandschutzsysteme, auf die Sie sich verlassen, alle einschlägigen Vorschriften erfüllen, wie z. B. die Produktnormen EN 54 und die länderspezifischen Regulative. Ein gut durchdachtes Brandmeldesystem ist intelligent und vollständig vernetzt, so dass bei einem Vorfall sofort die richtigen Maßnahmen automatisiert eingeleitet werden und Brände verhindert oder minimiert und Leben gerettet werden können. Das heutige Maß an Konnektivität und Automatisierung kennzeichnet intelligente Systeme und intelligente Gebäude, ermöglicht aber auch die ständige Gefahr von Cyberangriffen.

In diesem Dokument definieren wir "Cybersecurity" wie folgt:

"Der Schutz von Leben und Unternehmenswerten vor Schäden, die durch digitale Angriffe auf die Verfügbarkeit, Vertraulichkeit, Integrität, Authentizität und Zuverlässigkeit von Informationen im Cyberspace entstehen. Der "Cyberspace" ist das komplexe System der Interaktion zwischen Menschen, Software und Diensten, das durch den Einsatz technischer Mittel zur Verbindung mit dem Intranet und dem Internet ermöglicht wird."

Im Laufe der Zeit haben sich die Gebäudesysteme dramatisch verändert. Es fand ein Paradigmenwechsel von eigenständigen zu integrierten Systemen statt. Brandschutzsysteme bilden dabei keine Ausnahme. Nicht nur, dass vormals getrennte Brandschutztechnologien in ein einziges Netzwerk integriert werden, um die Reaktion auf Notfälle zu optimieren, auch die Brandschutzsysteme selbst werden mit anderen Gebäudesystemen wie HLK, Sicherheit, Aufzügen und Gebäudeautomation integriert. Diese Integration ermöglicht eine nahtlose Kommunikation zwischen diesen Systemen und eine kontinuierliche Überwachung im gesamten Gebäude. Diese Systemintegration verbessert die Sicherheit, erhöht die Kontrolle und den Komfort, reduziert Fehlalarme und spart Geld.

Gleichzeitig macht die Systemintegration robuste Cybersicherheit zu einer Notwendigkeit, nicht zu einem Luxus. Der Zugriff auf integrierte Systeme erfolgt zunehmend über Managementsysteme und Remote-Plattformen. Der Fernzugriff erleichtert die Verwaltung von Notfalleinsätzen sowie die Steuerung und Reparatur von Systemen, birgt aber auch Sicherheitsrisiken. Brandschutzsysteme könnten manipuliert und somit als Zugang zu weiteren Systemen ausgenutzt werden. Wenn integrierte Systeme über einen der Kommunikationswege angegriffen werden, stehen Leben und die Sicherheit von Werten auf dem Spiel.

Um die Sicherheit in der vernetzten Welt zu erhöhen, ist es wichtig, die Cybersicherheit ganzheitlich zu betrachten. In diesem Beitrag werden die Auswirkungen der Cybersicherheit auf Brandschutzsysteme und der Ansatz von Siemens zu diesem Thema untersucht.

Alle Rechte vorbehalten | © Siemens Schweiz AG 2022

Einführung

Wir leben und arbeiten in einer spannenden Zeit. Es ist eine, die von Industrie 4.0 bestimmt wird - der Digitalisierung der Wirtschaft. Die Digitalisierung bietet zahlreiche Vorteile, darunter mehr Komfort und höhere Effizienz. Sie bringt aber auch Herausforderungen für die Sicherheit mit sich. Cyberangriffe sind eine ständige und zunehmende Bedrohung aufgrund der flächendeckenden Konnektivität, die die Digitalisierung ermöglicht. In der vernetzten Welt von heute ist die Wahrscheinlichkeit eines Cyberangriffs hoch.

Wie können Sie Cyber-Bedrohungen selbstbewusst begegnen und sie minimieren? Sie verfolgen einen ganzheitlichen Ansatz für Sicherheitsmaßnahmen in allen Bereichen Ihres Unternehmens.

Bei Siemens Smart Infrastructure beginnt die Cybersicherheit bereits bei der Produktentwicklung. Bei der Entwicklung unserer Branderkennungsprodukte, -lösungen und -services haben wir eine "Think Security"-Philosophie verfolgt. Dieses Dokument gibt einen Einblick in die Art und Weise, wie Siemens die Anforderungen an die Cybersicherheit während der Produktentwicklung und des Lebenszyklusmanagements angeht.

Bevor wir über Cybersicherheit sprechen, sollten wir sie definieren. In diesem Dokument definieren wir "Cybersecurity" als den Schutz von Leben und Unternehmenswerten vor Schäden, die durch digitale Angriffe auf die Verfügbarkeit, Vertraulichkeit, Integrität, Authentizität und Zuverlässigkeit von Informationen im Cyberspace entstehen. Der "Cyberspace" ist das komplexe System der Interaktion zwischen Menschen, Software und Diensten, das durch den Einsatz technischer Mittel zur Verbindung mit dem Intranet und dem Internet ermöglicht wird. Lassen Sie uns auch definieren, was es bedeutet, einen ganzheitlichen Sicherheitsansatz zu verfolgen. Führende Unternehmen und Institutionen berücksichtigen vier Schlüsselfaktoren, die sich auf die Stärke der Sicherheit auswirken: Menschen, Kommunikation, Prozesse und Technologie. Ganz allgemein:

- Die Menschen brauchen ein breites und dauerhaftes Bewusstsein für die Bedeutung der Sicherheit, sowohl der physischen Sicherheit als auch der Cybersicherheit.
- Eine klare, kurze und präzise Kommunikation trägt dazu bei, eine Sicherheitskultur zu schaffen.
- Aktiv angewandte Verfahren sind für den Schutz von Unternehmen vor Cyber-Bedrohungen ebenso wichtig wie Technologien.
- Technologie muss getestet, geprüft und mit anderen geeigneten Bausteinen kombiniert werden, um die IT- und OT-Infrastruktur einer Organisation zu schützen.

Das Spektrum der Sicherheitsherausforderungen ist breit gefächert. Während physische Bedrohungen offensichtlicher sind und sich seltener ändern, können Cyber-Herausforderungen aufgrund einer sich ständig verändernden Bedrohungslandschaft hinterhältiger sein. Wenn es darum geht, die Sicherheit mit den geschäftlichen Anforderungen und dem unvermeidlichen Trend zur Bequemlichkeit in Einklang zu bringen, legen wir von Anfang an einen Schwerpunkt auf die Cybersicherheit.

Alle Rechte vorbehalten | © Siemens Schweiz AG 2022

Smarter Brandschutz ist das Herzstück jedes smarten Gebäudes

Der Brandschutz ist für große und kleine Gebäude, vom Kindergarten bis zum Kraftwerk, von größter Bedeutung. Siemens ist seit 1851, als unser Unternehmen in Berlin die erste elektrische Brandmeldeanlage Europas installierte, führend bei der Entwicklung innovativer Lösungen, die Leben, Werte und Geschäftskontinuität besser schützen. Heute verfügen wir über Systeme, die alle wichtigen Elemente des Brandschutzes auf intelligente Weise zusammenführen und Ihren spezifischen Anforderungen gerecht werden.

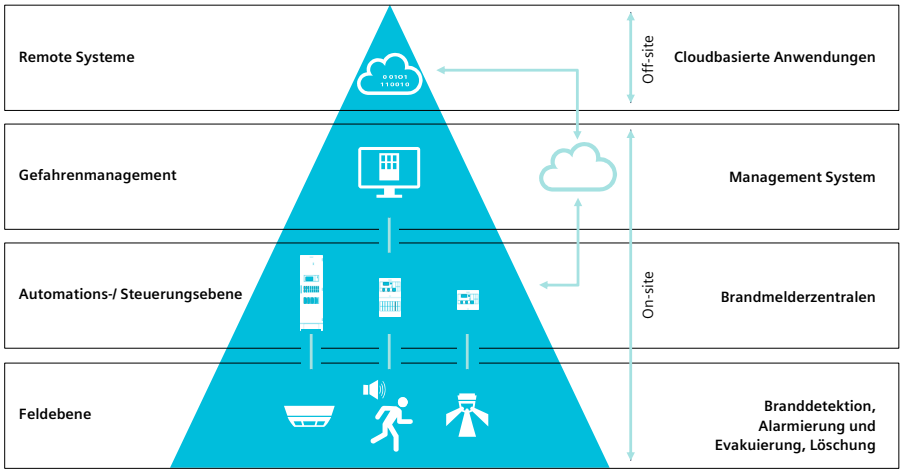
Siemens Systeme führen alle wichtigen Elemente des Brandschutzes auf intelligente Weise zusammen und werden Ihren spezifischen Anforderungen gerecht.

Das Ergebnis ist ein smarter Brandschutz:

- Detektion: Je früher Sie von einem Brand erfahren, desto schneller können Sie ihn bekämpfen. Unsere leistungsstarken, einfach zu bedienenden Brandmeldezentralen und täuschungsfreien Brandmelder erkennen Gefahrensituationen schnell und mit unschlagbarer Genauigkeit.
- Alarmierung, Benachrichtigung und Evakuierung: Ein gut geplantes und gesteuertes Vorgehen alarmiert und benachrichtigt die Menschen, ohne sie in Panik zu versetzen, und führt sie geordnet an einen sicheren Ort.
- Löschung: Wir bieten Ihnen genau die Löschlösung, die Sie brauchen, um einen Brand in Ihrem Gebäude schnell zu löschen, bevor er Menschenleben bedroht oder wertvolle Werte wie Daten oder unersetzliche Museumsobjekte zerstört.
- Gefahrenmanagement: Die gleichzeitige Verwaltung von Brandschutz, physischer Sicherheit und Gebäudeautomationssystemen bei kritischen Ereignissen gibt Ihnen mehr Möglichkeiten, schneller und zuverlässiger zu reagieren. Unser Gefahrenmanagement-Portfolio ist einfach zu bedienen, zu warten und zu pflegen.
- Cloud-Konnektivität: Unsere Cloud-Plattformen bieten gesicherte Remote-Konnektivität und Datenaustausch, die die Service-Effizienz erhöhen.

Alle Rechte vorbehalten | © Siemens Schweiz AG 2022

Mit jedem neuen Brandmeldesystem oder Update, das Siemens entwickelt, wird unsere Technologie intelligenter und leistungsfähiger und verfügt über zusätzliche innovative Geräte und Funktionen. Um sicherzustellen, dass jedes System das ganze Jahr über ein hohes Maß an Schutz für wertvolle Einrichtungen bietet, haben wir mehrere Redundanzebenen sowie eine umfassende Selbstüberwachung und -prüfung eingebaut. Sie können sich auf unsere Erfahrung und unseren Einfallsreichtum verlassen, um eine Lösung zu erhalten, die heute den bestmöglichen Brandschutz bietet und morgen problemlos erweitert werden kann, wenn sich Ihre Anforderungen ändern.



Siemens-Lösungen bieten bestmöglichen Brandschutz.

"Security by Design" ist unser durchgängiger Ansatz bei der Produktentwicklung, der Sicherheit von Anfang an einbezieht.

“Security by Design:” Siemens engagiert sich für umfassende Sicherheit

Cyberangriffe gehören heute zu den am schnellsten wachsenden kriminellen Aktivitäten in der Welt. Sie reichen von Insider-Bedrohungen, Ransomware-Angriffen, opportunistischen Bedrohungen und Hacktivismus bis hin zu Wirtschaftsspionage, Terrorismus und staatlich gesponsertem Cyberterrorismus. Um auf eine schnelle, komplexe und sich ständig verändernde Bedrohungslandschaft vorbereitet zu sein, ist es unerlässlich, dass Unternehmen wie das Ihre eine umfassende Verteidigung entwickeln.

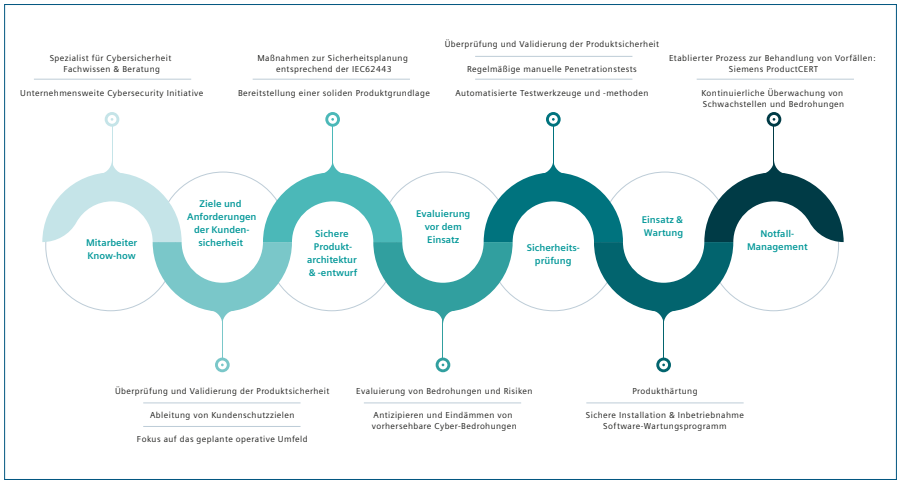
Während die Verantwortung für die Sicherung Ihrer Umgebung bei Ihrem Unternehmen liegt, engagiert sich Siemens für die Entwicklung von Produkten, die Ihnen einen ganzheitlichen Sicherheitsansatz ermöglichen. Dies gilt für unser breites Portfolio an Produkten, Lösungen und Dienstleistungen für die Gebäudetechnik.

Unser Engagement ist vielschichtig. An erster Stelle steht "Security by Design", unser durchgängiger Ansatz bei der Produktentwicklung, der Sicherheit von Anfang an einbezieht. Dazu gehört ein ständiger Zyklus von Tests, Verbesserungen und Weiterentwicklungen, um unsere Produkte und Lösungen auf dem neuesten Stand zu halten. Darüber hinaus sind wir Gründungsmitglied der globalen Charta of Trust,[1] die verbindliche Regeln und Standards fordert, um das Vertrauen in die Cybersicherheit zu stärken und die Digitalisierung voranzutreiben.

[1] Weitere Informationen finden Sie unter www.charteroftrust.com.

Alle Rechte vorbehalten | © Siemens Schweiz AG 2022

Einfach ausgedrückt: Wir entwickeln mit Fokus auf die Sicherheit. Unsere unternehmensweite Initiative beinhaltet ein Risikomanagementprogramm, das eine umfassende Sicherheitsmethodik für alle Siemens-Produkte, -Lösungen und -Services aktiv vorantreibt. Es identifiziert Best Practices und legt technische Standards, Prozesse und Richtlinien fest, die eingehalten werden müssen. Wir tragen auch zu internationalen Standards bei und bemühen uns, Produkte zu liefern, die Sicherheitsstandards wie ISA/IEC 62443, UL2900, ISO/IEC 27001 und OWASP erfüllen.



Siemens Cybersecurity Initiative Highlights

Während des gesamten Lebenszyklus des Produkts führen unsere Experten Sicherheits- und Risikobewertungen durch.

Security by Design Expertise

Die Wirksamkeit des Cybersicherheitskonzepts eines Produkts ist auf die Kompetenz des Entwicklungsteams zurückzuführen. Im Rahmen unserer "Security by Design"-Methode investieren wir nicht nur in technologische Entwicklungen für den digitalen Schutz und die Produktsicherheit, sondern auch in die Schulungen, die erforderlich sind, um ein hohes Maß an Cybersicherheits-Know-how der Mitarbeiter zu gewährleisten.

Während des gesamten Lebenszyklus des Produkts führen unsere Experten Sicherheits- und Risikobewertungen durch, um das erwartete Risiko in der vorgesehenen Anwendung zu berücksichtigen. Diese Bewertung beginnt bereits in einem frühen Stadium des Prozesses und wird bei Bedarf wiederholt, um Risiken zu erkennen und angemessen zu entschärfen.

Darüber hinaus werden regelmäßige Produkt-Sicherheitstests von externen Experten durchgeführt, die manuelle Penetrationstests allein oder in Kombination mit automatisierten maschinellen Sicherheitstests verwenden. Das Ziel ist es, das System zu brechen, um es sicherer zu machen. Durch diese Tests wird sichergestellt, dass das ausgewählte Produkt, die Lösung oder die Dienstleistung unseren Sicherheitsanforderungen entspricht. Die Testergebnisse werden aufgezeichnet und zur Ermittlung notwendiger Korrekturmaßnahmen verwendet.

“Security by Default”

Das Konzept "Security by Default" ist eng mit dem Konzept "Security by Design" verbunden. Es sieht vor, dass alle Schutzmaßnahmen zum Zeitpunkt der Produk-

tauslieferung, Installation oder Erstinbetriebnahme automatisch aktiviert und standardmäßig in Kraft treten. Security by Default wird heute immer häufiger angewandt, um der Tatsache entgegenzuwirken, dass viele Entwickler Software mit weit offenen Einstellungen ausgeliefert haben, weil sie davon ausgingen, dass die Benutzer die Sicherheit bei der Einrichtung konfigurieren würden. Leider denken die meisten Benutzer nicht an die Sicherheit, wenn die Software bereits läuft. Damit die Sicherheit effektiv funktioniert, muss sie vom ersten Tag an eingebaut und aktiv sein. Darüber hinaus ist es schwierig, nachträglich hinzugefügte Sicherheitsfunktionen zu patchen oder nachzurüsten, wenn neue Angriffsmethoden entdeckt werden.

Security by Default ist zwar auf dem Vormarsch, doch gibt es derzeit keine einheitlichen Vorschriften für diesen Ansatz. Daher werden geeignete Sicherheitseinstellungen oft nicht im Voraus festgelegt, so dass die Benutzer sie nach der Installation des Produkts anpassen müssen. Siemens hingegen entwickelt und konfiguriert seine Systeme so, dass die sichersten Einstellungen bei der Installation standardmäßig verwendet werden. Bei der Entwicklung setzen wir das höchste angemessene Sicherheits- und Datenschutzniveau an und integrieren es in das Design des Produkts, die Funktionalitäten, die Prozesse und den Betrieb. Schließlich sorgen wir dafür, dass die eingebetteten Sicherheitsmaßnahmen sofort aktiviert werden, wenn das System in Betrieb genommen wird.

Damit "Security by Default" erfolgreich ist, muss die Frage untersucht werden, wie Produkte ein hohes Maß an Sicherheit bieten können, wenn sie das Werk verlassen. Bekannte Beispiele für Schwachstellen im realen Leben zeigen, dass viele Unternehmen ein leichtes Ziel für böswillige Akteure wurden. Bei einem der ungewöhnlichsten Vorfälle hackten sich Cyberkriminelle über ein mit dem Internet verbundenes Thermometer in einem Aquarium in der Lobby eines Kasinos ein.[2] Dadurch erhielten die Hacker Zugang zum Kasinonetzwerk und zur Datenbank der Spieler mit hohen Einsätzen, die sie in die Cloud hochluden. Manche Lösungen sind einfacher als andere. Um ein angemessenes Sicherheitsniveau vor Ort aufrechtzuerhalten, sollte es eine strenge Empfehlung geben, die die Erstellung eines neuen Passworts verlangt, wenn sich der Benutzer erstmals anmeldet. Aber welche weiteren Sicherheitsmaßnahmen müssen in Betracht gezogen werden und welche Kompromisse können im Interesse der Benutzerfreundlichkeit eingegangen werden? Einfache, allgemeingültige Antworten, geschweige denn konkrete Handlungsempfehlungen, gibt es bisher nicht. Stattdessen werden die Maßnahmen von den zuständigen Produktteams entwickelt. Das Signal ist jedoch eindeutig: Cybersicherheit ist nicht mehr optional. Sie ist jetzt eine Pflichtaufgabe.

[2] Weitere Informationen finden Sie unter
https://www.forbes.com/sites/leemathews/2017/07/27/criminals-hacked-a-fish-tank-to-steal-data-from-a-casino/

Alle Rechte vorbehalten | © Siemens Schweiz AG 2022

Eine sorgfältige Zuweisung von Zugriffsrechten entsprechend den jeweiligen Aufgaben kann den Schaden sowohl durch die Systembenutzer als auch durch potenzielle Hacker begrenzen.

"Principle of Least Privilege"

Das Principle of Least Privilege ist seit seiner Einführung durch Jerome Saltzer und Michael Schroeder im Jahr 1975 ein Grundpfeiler der Informationssicherheit.[3] Es basiert auf dem Konzept, dass eine sorgfältige Zuweisung von Zugriffsrechten entsprechend den jeweiligen Aufgaben den Schaden sowohl durch die Systembenutzer als auch durch potenzielle Hacker begrenzen kann. Es sieht vor, dass autorisierte Benutzer eines Systems so wenig wie möglich und so kurz wie möglich Zugriffsrechte haben, um ihre Arbeit zu erledigen. Es kann auch dazu verwendet werden, die Anzahl der möglichen Interaktionen zu begrenzen, so dass eine unbeabsichtigte, unerwünschte oder unsachgemäße Nutzung von Privilegien weniger wahrscheinlich ist. Wenn es richtig angewendet wird, hilft das Principle of Least Privilege dabei, den Schaden zu verhindern, der durch ein Versehen oder einen Fehler eines Benutzers entstehen kann, und es hilft dabei, die Möglichkeiten eines Hackers auf der Grundlage des kompromittierten Benutzerkontos zu begrenzen.

Das Principle of Least Privilege ist auf jeder Ebene eines Systems und für jeden Benutzer, jede Datenbank und jeden Prozess hilfreich. Wir wenden es auf unsere Systeme an, indem wir den Zugriff auf Daten und Anwendungen auf das für eine bestimmte Aufgabe erforderliche Minimum beschränken. Dies ist im Falle eines erfolgreichen Cyberangriffs von entscheidender Bedeutung, da der Hacker die Rechte des Benutzerkontos erhält, auf das er Zugriff hat. Erfolgt ein Angriff über das Konto eines Mitarbeiters mit administrativen Rechten, kann sich eine Infektion systemweit ausbreiten. Daher sollte ein Benutzer, der keinen administrativen Zugriff benötigt, wann immer es angebracht ist, mit weniger Privilegien und begrenztem Umfang arbeiten. Außerdem ist es wichtig, dass technische Benutzer nur über die Mindestberechtigungen verfügen, die für den Zugriff auf die Ressourcen, an denen sie arbeiten, erforderlich sind, und nicht über mehr. Wenn das Konto eines technischen Benutzers kompromittiert wird, kann ein Hacker die zugewiesenen Berechtigungen missbrauchen, um unerwünschte Aktivitäten durchzuführen, wie z. B. das Löschen einer ganzen Datenbank oder die Installation von Malware.

[3] Smith, Richard E. "A Contemporary Look at Saltzer and Schroeder's 1975 Design Principles," IEEE Security & Privacy, Volume 10, Issue 6, Nov.-Dec. 2012.

Alle Rechte vorbehalten | © Siemens Schweiz AG 2022

Teilen Sie kritische Funktionen auf verschiedene autorisierte Benutzer auf, um das Risiko von Betrug und anderen Missbräuchen zu minimieren.

"Separation of Duties Principle"

Ein weiteres IT-Sicherheitskonzept, das eng mit dem Principle of Least Privilege verbunden ist, ist das Separation of Duties Principle. Es teilt kritische Funktionen auf verschiedene autorisierte Benutzer auf, um das Risiko von Betrug und anderen Missbräuchen durch Mitarbeiter oder andere autorisierte Personen zu minimieren. Es besagt, dass kein Benutzer genügend Privilegien erhalten sollte, um das System auf eigene Faust zu missbrauchen. Die Aufgabentrennung kann entweder durch die Definition von Rollen, die nicht von ein und demselben Benutzer ausgeführt werden können, oder durch die Durchsetzung des Vier-Augen-Prinzips beim Zugriff durchgesetzt werden. In letzterem Fall kann die erste Person, die einen Vorgang mit zwei Personen ausführt, ein beliebiger autorisierter Benutzer sein, während die zweite Person ein anderer autorisierter Benutzer sein muss.

Im Rahmen unseres ganzheitlichen Ansatzes für die Cybersicherheit unserer Angebote wenden wir das Principle of Least Privilege an, um den gesamten Lebenszyklus eines Systems zu berücksichtigen, vom Entwurf über die Inbetriebnahme und den Betrieb bis hin zur Migration und Stilllegung. Direkte Vorteile der Anwendung dieses Prinzips sind eine bessere Sicherheit und eine minimale Angriffsfläche. Darüber hinaus können sich zusätzliche Vorteile in Bezug auf Stabilität, Rückverfolgbarkeit und andere ressourcenabhängige Dienste ergeben.

ISA/IEC 62443

Digitalisierung und Cybersicherheit sind zwei eng miteinander verknüpfte Themen, die für Unternehmen auf der ganzen Welt von großer strategischer Bedeutung sind. Wenn es um die Cybersicherheit unseres Portfolios geht, verfolgt Siemens einen umfassenden Ansatz, der sich an internationalen Standards orientiert.

Einer der wichtigsten Standards ist ISA/IEC 62443, der von der International Society of Automation (ISA) entwickelt und von der International Electrotechnical Commission (IEC) übernommen wurde. ISA/IEC 62443 hat sich im Umfeld der industriellen Automatisierung bewährt. Sie richtet sich an Anlagenbetreiber, Integratoren und Komponentenhersteller und deckt die dringenden sicherheitsrelevanten Aspekte der industriellen Sicherheit ab.

Alle Rechte vorbehalten | © Siemens Schweiz AG 2022

Siemens Smart Infrastructure Building Products ist nach IEC 62443-4-1 mit Reifegrad 3 zertifiziert. Diese Zertifizierung ist Voraussetzung für die Zertifizierung eigener Produkte, d.h. für die Erlangung der IEC 62443-4-2 Produktzertifizierung und den Aufbau cybersicherer Brandmeldeanlagen.

Wir betten Cybersicherheitsmaßnahmen in unsere Produkte ein und suchen kontinuierlich nach Sicherheitsverbesserungen, die die Widerstandsfähigkeit gegen Cyberangriffe weiter erhöhen.

Anwendung von Security by Design auf Sinteso EN Brandschutzsysteme

Unsere Familie von robusten, innovativen und modernen Brandmeldesystemen trägt dazu bei, sichere Umgebungen für Menschen und Anlagen zu schaffen und gleichzeitig die Geschäftskontinuität zu verbessern. In den letzten Jahren wurden Brandmelderanlagen immer stärker mit anderen Gebäudesystemdisziplinen vernetzt, wodurch die Fernkonnektivität zu einem wichtigen Trend und Vorteil in der Gebäudeautomationsbranche wurde. Fernkonnektivität bedeutet jedoch auch, dass die Bedrohungen durch Cyberangriffe in den letzten Jahren zugenommen haben. Der Brandschutz ist dagegen nicht immun. Um diesen Bedrohungen entgegenzuwirken, haben wir 2015 mit der Implementierung neuer Cybersicherheitsmaßnahmen begonnen und die Cybersicherheit unserer Brandschutzsysteme mit jeder neuen Version erhöht.

In Anlehnung an die Cybersicherheitsnorm IEC 62443 und die Charta of Trust haben wir den ganzheitlichen Security-by-Design-Gedanken in unseren Produktentwicklungsprozess für Brandschutzsysteme integriert. Durch die Anwendung der IEC 62443 betten wir Cybersicherheitsmaßnahmen in unsere Produkte ein und suchen kontinuierlich nach Sicherheitsverbesserungen, die die Widerstandsfähigkeit von Brandschutzsystemen gegen Cyberangriffe weiter erhöhen. So haben wir beispielsweise gehärtete Fernzugriffsfunktionen für eine sicherere Cloud-Kommunikation eingeführt.

Um den Erwartungen an die Cybersicherheit gerecht zu werden, wird jede neue Version unserer Brandschutzsysteme Penetrationstests unterzogen und jede cybersicherheitsrelevante Funktion einer Bedrohungs- und Risikoanalyse unterzogen.

Alle Rechte vorbehalten | © Siemens Schweiz AG 2022

Unsere Experten halten sich an die unternehmensweite Cybersicherheitsinitiative von Siemens. Sie befolgen die verbindliche interne Sicherheitsrichtlinie, die Maßnahmen für die Weiterentwicklung, Inbetriebnahme und den Service von Brandmeldeprodukten in Übereinstimmung mit den entsprechenden Benutzerrollen und Sicherheitsstufen beim Kunden vorsieht.

Diese Maßnahmen tragen dazu bei, dass die Codierung zu einer sichereren Implementierung von Brandmeldekomponenten führt. Dazu gehört auch, dass bestimmte Merkmale und Funktionen standardmäßig sicherer gemacht werden. Und da wir unsere Produkte, Lösungen und Dienstleistungen kontinuierlich verbessern und weiterentwickeln, können wir den Schutz unserer Brandmeldesysteme verfeinern, wenn neue Sicherheitsbedrohungen auftreten.

Und da wir unsere Produkte, Lösungen und Dienstleistungen kontinuierlich verbessern und weiterentwickeln, können wir den Schutz unserer Brandmeldesysteme verfeinern, wenn neue Sicherheitsbedrohungen auftreten.

Beispiele für "Security by Design"-Elemente, die in die Sinteso Brandschutzsystemfamilie integriert werden, sind:

- Cybersecurity Richtlinien für den sicheren Einsatz von EN 54 Brandmeldeanlagen
- Authentifizierung von Inbetriebsetzungs- und Servicetools
- Firmware Watchdogs
- Erweiterter Audit Trail
- Ereignis- / Alarm-Log
- Systemlog
- Härten von Brandmeldeanlagen
- Kontinuierliche Upgrades des Betriebssystems
- Erweiterung der Authentifizierung
- Härten von Inbetriebsetzungs- und Servicetools
- Regelmässige Penetrationstests und Gefahren- und Risikoanalysen
- Firmware Signaturen
- Integration der Verfügbarkeit von Brandmeldesystemen in einer Cyber-Secure Architektur
- Verwendung verifizierter 3rd Party Komponenten
- Eindeutige Identifizierung von Geräten und Komponenten der Brandmeldetechnik
- Integrierte und gesicherte Cloud-Verbindung
- Unterstützung von physikalisch getrennten Brandmeldenetzwerken

Alle Rechte vorbehalten | © Siemens Schweiz AG 2022

Sicherstellung von Cybersicherheit bei Sinteso Brandschutzsysteme

Wir veröffentlichen Richtlinien zur Cybersicherheitshärtung, um die sichere Inbetriebnahme und den Einsatz unserer Brandschutzsysteme zu unterstützen. Diese Richtlinien beschreiben, wie unsere Systeme, Produkte und Lösungen für einen sicheren Betrieb in der vorgesehenen Umgebung konfiguriert werden müssen. Zu den Konfigurationsoptionen gehören beispielsweise die zu installierenden Anwendungen, die zu aktivierenden oder deaktivierenden Einstellungen, Firewall-Konfigurationen und die Festlegung von Zugriffsrechten. Die Härtungsrichtlinien werden während des gesamten Lebenszyklus des Produkts beibehalten.

Im Rahmen unseres Wartungsprogramms veröffentlichen wir regelmäßig Upgrades, die neue bekannte Schwachstellen beseitigen und den Schutz unserer Brandschutzsysteme vor Bedrohungen erhöhen. Die neuesten Informationen zur Cybersicherheit unserer Brandmeldeanlagen finden Sie in unserer Dokumentation und in unserem Kundendienstzentrum.

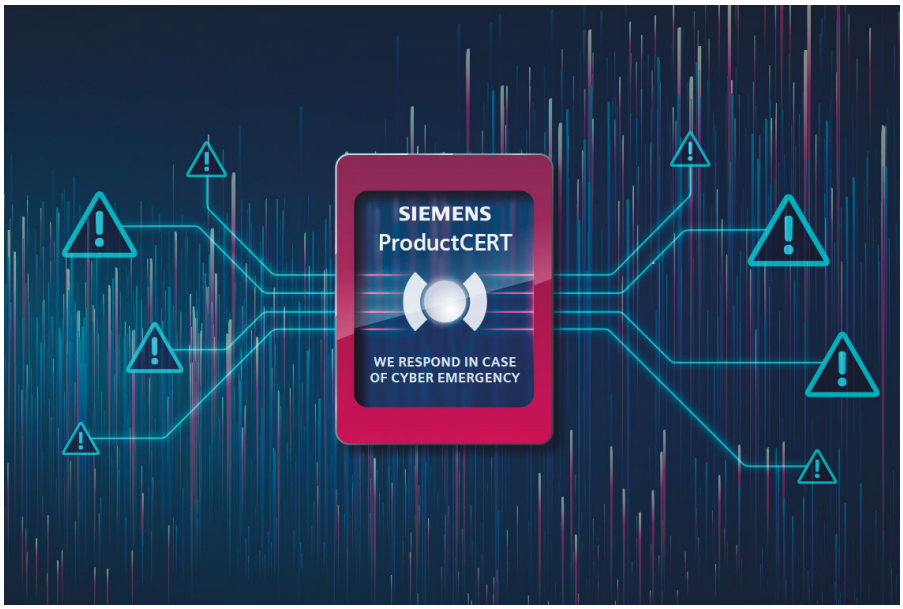
Sinteso Produktfamilie

Remote Services

Der Fernzugriff ist heutzutage eine wünschenswerte Funktion, da er eine ständige Leistungsüberwachung und Bequemlichkeit bietet. Unsere Brandschutzsysteme sind darauf vorbereitet, Dienste zu unterstützen, die auf Datenfernzugriff angewiesen sind, während sie gleichzeitig Teil des Sicherheitskonzepts der Umgebung bleiben. Durch die Unterstützung von Remote-Diensten ermöglicht Ihnen unsere Familie von Brandmelderanlagen den Zugriff auf Daten über Ihre Brandmelderanlagen und angeschlossenen Geräte, so dass Sie Ihren Betrieb optimieren können.

Während der Fernzugriff über Ihre Standard-IT-Mechanismen möglich ist, nutzen wir unsere Cloud-Konnektivität oder die Siemens Common Remote Service Plattform (cRSP) für einen noch sichereren Fernzugriff. Unser zuverlässiger und leistungsfähiger Fernzugriff ermöglicht den weltweiten Zugriff auf Daten und Informationen im Zusammenhang mit Ihrer Brandschutzinfrastruktur. Die Siemens cRSP ist konform mit ISO/IEC 27001 - der Norm für systematisches Cybersecurity-Management auf Organisationsebene. Diese Plattform stellt sicher, dass die von Siemens bereitgestellten Remote-Services die strengen Anforderungen an die Cybersicherheit erfüllen.

Alle Rechte vorbehalten | © Siemens Schweiz AG 2022



Notfall-Management

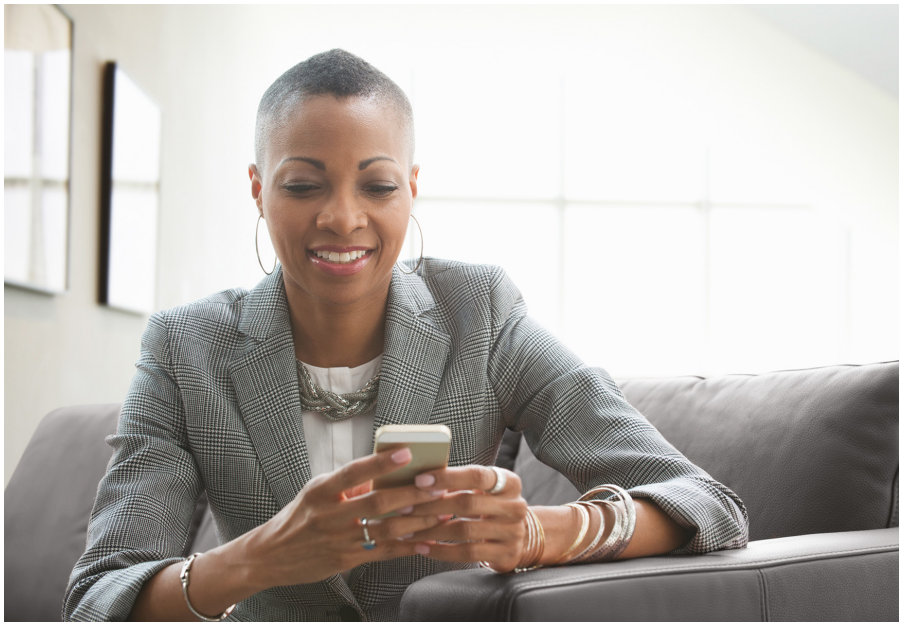
Für unsere Angebote haben wir Prozesse zur Behandlung von Incidents und Vulnerabilities für den Fall eingerichtet, dass ein Sicherheitsproblem oder eine Schwachstelle in unseren Brandschutzsystemen entdeckt wird.

Prozess zur Behandlung von Zwischenfällen und Schwachstellen: Unser Support-Mechanismus für von Kunden gemeldete Sicherheitsprobleme folgt einem vierstufigen Prozess, der Meldung, Analyse, Bearbeitung und Offenlegung umfasst. Schwachstellen und/oder Vorfälle werden an unser technisches Support-Team weitergeleitet, das durch das globale Siemens ProductCERT-Team unterstützt wird, das rund um die Uhr im Einsatz ist. Es werden die notwendigen Schritte eingeleitet, um die Situation zu bewältigen, und die Vorfälle und Abhilfemaßnahmen werden bekannt gegeben.

Schwachstellen-Management: Dies ist unser interner Erkennungsprozess zur Feinabstimmung des Sicherheitsniveaus unserer Produkte und Lösungen. Die kontinuierliche Überwachung von Bedrohungen ermöglicht es uns, potenzielle Schwachstellen in unseren Produkten und Lösungen zu erkennen und zu entschärfen. Die Software-Komponenten in unseren Brandmelderanlagen werden registriert, so dass beim Auftreten von Sicherheitslücken die erforderlichen Abhilfemaßnahmen ergriffen und bekannt gegeben werden können. Identifizierte Schwachstellen werden vom ProductCERT-Team über die ProductCERT-Sicherheitshinweise (https://new.siemens.com/global/en/products/services/cert.html) bekannt gegeben, die Sie abonnieren können.

Alle Rechte vorbehalten | © Siemens Schweiz AG 2022

Zusammenfassung



Als Marktführer in der Gebäudetechnik und bei Brandschutzsystemen kennen wir die Herausforderungen, denen Sie bei der Erfüllung Ihrer Cybersicherheitsanforderungen in der heutigen Welt gegenüberstehen. Unser umfassendes Sicherheitskonzept für den gesamten Produktlebenszyklus bedeutet, dass unsere Brandschutzsystemfamilie mit Blick auf Ihre Sicherheit entwickelt wird. Sie können sich auf unsere Erfahrung und unseren Einfallsreichtum verlassen, wenn es darum geht, eine Lösung zu finden, die Ihnen hilft, das zu schützen, was Ihnen wichtig ist - eine Aufgabe, die Siemens seit der Installation der ersten elektrischen Brandmeldeanlage in Europa im Jahr 1851 wahrnimmt.

Unser Team setzt sich für die Sicherheit Ihrer Mitarbeiter, Anlagen, Vermögenswerte und die Kontinuität Ihres Geschäftsbetriebs ein. Intelligente Unternehmen machen Sicherheit zu einem der Eckpfeiler ihres Geschäftsmodells.

Alle Rechte vorbehalten | © Siemens Schweiz AG 2022

Cybersicherheits-Haftungsausschluss

Siemens offeriert ein Portfolio von Produkten, Lösungen, Systemen und Dienstleistungen mit Sicherheitsfunktionen, die den sicheren Betrieb von Anlagen, Systemen, Maschinen und Netzwerken unterstützen. Im Geschäftsfeld der Gebäudetechnik umfasst dies Systeme für Gebäudeautomation und -leittechnik, Brandschutz, Sicherheitsmanagement und physische Sicherheitssysteme.

Um Anlagen, Systeme, Maschinen und Netzwerke vor Online-Bedrohungen zu schützen, ist es erforderlich, ein ganzheitliches, dem neuesten Stand der Technik entsprechendes Sicherheitskonzept zu implementieren und stets auf dem aktuellen Stand zu halten. Das Portfolio von Siemens bildet nur einen Bestandteil eines solchen Konzeptes.

Sie als Betreiber einer Brandmelderzentrale, sind dafür verantwortlich, unbefugten Zugang zu Ihren Anlagen, Systemen, Maschinen und Netzwerken zu verhindern. Diese sollten nur mit einem Netzwerk oder dem Internet verbunden werden, wenn und soweit die Verbindung erforderlich ist und angemessene Sicherheitsvorkehrungen (z. B. Firewalls bzw. Netzwerksegmentierung) vorhanden sind. Darüber hinaus sind die Sicherheitsempfehlungen von Siemens zu beachten. Für nähere Informationen kontaktieren Sie bitte Ihren Ansprechpartner bei Siemens oder besuchen Sie unsere Webseite https://new.siemens.com/global/en/products/automation/topic-areas/industrial-security.html.

Zur Verbesserung der Sicherheit wird das Portfolio von Siemens kontinuierlich weiterentwickelt. Siemens empfiehlt dringend, Updates zu installieren, sobald diese zur Verfügung stehen, und stets die neusten Versionen zu verwenden. Werden Versionen verwendet, die nicht mehr unterstützt werden, oder werden die neuesten Updates nicht verwendet, kann sich Ihr Risiko bezüglich Online-Bedrohungen erhöhen. Siemens empfiehlt dringend, Sicherheitsempfehlungen zu den neuesten Sicherheitsgefährdungen, Patches und damit verbundenen Maßnahmen zu befolgen, die unter anderem unter https://new.siemens.com/global/en/products/services/cert.html veröffentlicht werden.

Herausgeber
Siemens Schweiz AG

Smart Infrastructure
Global Headquarters
Theilerstrasse 1a
6300 Zug
Switzerland
Tel +41 58 724 24 24

Artikel-Nr. SI_0208_DE (Stand 9/2022)

Änderungen und Irrtümer vorbehalten. Die Informationen in diesem Dokument enthalten lediglich allgemeine Beschreibungen bzw. Leistungsmerkmale, welche im konkreten Anwendungsfall nicht immer in der beschriebenen Form zutreffen bzw. welche sich durch Weiterentwicklung der Produkte ändern können. Die gewünschten Leistungsmerkmale sind nur dann verbindlich, wenn sie bei Vertragsschluss ausdrücklich vereinbart werden.

© Siemens 2022