genua.

Security by Design

Fast überall wird die Digitalisierung und Vernetzung vorangetrieben. Leider wachsen mindestens ebenso schnell die IT- und OT-Schwachstellen. Besonders kritisch: Diese finden sich häufig in Sicherheitsprodukten, die eigentlich dem Schutz dienen sollten. Daher gewinnt Security by Design zunehmend an Bedeutung. Es ist die Grundlage für resilientere Systeme und konkrete Maßnahmen, die Hersteller, Betreiber, Anwender und politische Entscheidungsträger ergreifen sollten.

SecurITy made in Germany

Kaum ein Tag vergeht ohne Meldungen über neue Schwachstellen in IT- und OT-Produkten, Diensten oder Infrastrukturen. Kaum ein Tag vergeht ohne Meldungen über neue erfolgreiche Angriffe oder Datenlecks in Industrie oder Verwaltung. Selbst Berichte über erfolgreiche Infiltration oder gar Sabotage kritischer Infrastrukturen in Deutschland durch ausländische Mächte sind nicht mehr ungewöhnlich. Und viel zu oft stecken die Schwachstellen auch in Sicherheitsprodukten, welche doch eigentlich vor Angriffen schützen sollten.

Die Erwartung ist daher, grundsätzlich nur noch Produkte einzusetzen, die über einen angemessenen Zeitraum mit Updates versorgt werden – und dass Anwender diese Sicherheitsupdates umgehend einspielen. Doch das ist keine umfassende Lösung: Denn Aktualisierungen können ihrerseits zum Problem werden.

Im besten Fall führen sie lediglich zu kurzen Betriebsunterbrechungen. Im schlimmsten Fall enthalten sie selbst Sicherheitslücken. Hinzu kommen immer ausgefeiltere Angriffe. Beispielsweise nutzen Angreifer bei sogenannten Zero-Day-Attacken Schwachstellen aus, bevor es Updates vom Hersteller gibt.

Gerade im industriellen OT-Umfeld werden Produkte deutlich über ihre offizielle Lebensdauer hinweg eingesetzt. Updates werden gar nicht oder verzögert eingespielt, da ständige Änderungen nicht mit einer stabilen und kontinuierlichen Produktion und ggf. einer behördlichen Zulassung der Anlagen vereinbar sind. Auch im IT-Umfeld führt die Vielfalt sowie die schiere Menge an Produkten und Schwachstellen dazu, dass sich viele Verantwortliche auf die vermeintlich kritischen Updates konzentrieren – und Restrisiken in Kauf nehmen.

Security by Design ist ein Lösungsansatz, mit dem sich solche Herausforderungen in den Griff bekommen lassen.

Dieses Whitepaper zeigt auf, wie es gelingt, Sicherheit tief im Design des Produkts zu verankern und dadurch für nachhaltige Sicherheit zu sorgen.

1. Mehr Digitalisierung, mehr Verantwortung

Digitale Lösungen sind heute ein starker Motor für die Produktivität. Sie spielen eine kritische Rolle für den Wettbewerb zwischen Unternehmen und zwischen Staaten. Allerdings geht die zunehmende Digitalisierung mit einer wachsenden Komplexität digitaler Produkte und Infrastrukturen einher. Das macht es für Hersteller und Anwender immer schwieriger, ihre Produktionsanlagen und Netzwerke sicher zu betreiben. Die Wahrscheinlichkeit von Fehlern und sicherheitskritischen Schwachstellen nimmt zu. Da nicht nur quantitativ mehr digitalisiert wird, sondern auch qualitativ, steigt zudem die Kritikalität der digitalisierten Daten und Prozesse.

In der Folge steht nicht selten nach einem Angriff das Überleben der gesamten Organisation auf dem Spiel. Unternehmen und Behörden mit hohem Schadpotenzial werden im Umkehrschluss sowohl für kriminelle als auch für fremdstaatliche Angreifer immer attraktiver. Wo viel auf dem Spiel steht, steigt die Aussicht auf eine hohe „Belohnung“. Kaum ein Tag vergeht ohne neue Berichte über Erpressung etwa durch Ransomware, Spionage oder Sabotage. Und je mehr und schneller digitalisiert wird, desto schneller wächst auch die Gefahr.

Inmitten dieser Situation werden die Anwender weitgehend allein gelassen. Hersteller und Dienstleister von digitalen Komponenten haften bis dato kaum für Schwachstellen in ihren Produkten.

Anbieter fokussieren sich auf sicht- und messbare Eigenschaften wie Features, Performance, Usability und Kosten. Wie sicher ein Produkt ist, ist für den Kunden hingegen überwiegend unsichtbar und damit kein vermarktbarer Wert, sondern ein störender Kostenfaktor für den Hersteller. Manche Anbieter werden erst aktiv, wenn ihre Reputation aufgrund offensichtlicher Mängel leidet.

Doch es gibt Ausnahmen: Nischen mit erhöhtem Schutzbedarf verlangen nach Zertifizierungen und Zulassungen für den Einsatz digitaler Produkte. Hier haben sich Hersteller auf die Bereitstellung von Lösungen mit nachweislich höherer Mindestsicherheit spezialisiert und entsprechende Kompetenzen aufgebaut. Diesem Vorbild folgend, darf die Verantwortung für Vorfälle mit unsicheren Produkten nicht länger ausschließlich bei den Anwendern liegen. Die Lieferanten müssen stärker in die Pflicht genommen werden. Durch bessere Produktqualität tragen sie unmittelbar zu einer höheren Sicherheit bei, was angesichts der zentralen Bedeutung digitaler Systeme für die wirtschaftliche und gesellschaftliche Stabilität ganzer Volkswirtschaften unverzichtbar ist.

Die Bedeutung hat mittlerweile auch die Politik erkannt. So liefert der Cyber Resilience Act (CRA) der Europäischen Union erste Ansätze auf regulatorischer Ebene. Ähnliche Bestrebungen gibt es auch in anderen Ländern. In den USA zeichnen sich erste Klagen ab, bei denen zum Nachteil der Kunden führende mangelnde Qualität bei IT-Produkten als grobe Fahrlässigkeit eingestuft wird. Dadurch können die üblichen vertraglichen Haftungseinschränkungen der Hersteller und Dienstleister aushebelt werden. Der CRA liefert zudem Ansätze, wie die nötigen Verbesserungen realisiert werden können: **Security by Design und Security by Default.**

2. Security by Design und Security by Default

Die Grundidee von Security by Design ist, Sicherheit früh in der Designphase zu berücksichtigen, statt sich auf eine nachträgliche Härtung des fertigen Produktes zu beschränken. Schwachstellen sollen von Beginn an proaktiv reduziert oder vermieden werden. Eine robuste Architektur soll zudem Fehler mitigieren, die bei komplexen Systemen unweigerlich auftreten. Security by Design steht für eine nachhaltige Produktentwicklung, die frühzeitig auf eine hohe inhärente Qualität fokussiert. Diese Philosophie steht im direkten Kontrast zu dem immer noch weit verbreiteten Motto „Ship first, fix later“.

Security by Default erweitert die Idee der inhärenten Sicherheit über die Architektur hinaus: Der Anwender soll nicht länger verpflichtet sein, das Produkt vor der Nutzung erst einmal sicher zu konfigurieren – es muss bereits bei der Auslieferung sicher sein! Sofern die Einsatzumgebung später unsichere Anpassungen nötig macht, sollte der Anwender diese nur explizit und im Bewusstsein der damit einhergehenden Risiken vornehmen.

„Der Security-by-Design-Ansatz eignet sich auch für den Aufbau von IT-Infrastrukturen.“

Auch wenn Security by Design und Security by Default heute primär für die Softwareentwicklung propagiert werden, steigt die Bedeutung dieser Prinzipien auch beim Aufbau von IT-Infrastrukturen und selbst bei der Gestaltung von Arbeitsprozessen. Denn das nachträgliche Hinzufügen von Sicherheitsmaßnahmen ist nicht nur wenig effizient und häufig weniger effektiv, sondern behindert Anwender deutlich stärker als eine frühzeitig und mit Bedacht integrierte Sicherheit.

Um Security by Design und Security by Default nachhaltig umzusetzen, bedarf es ausreichender Expertise und einer entsprechenden Firmenkultur. Sowohl die zu adressierenden Risiken als auch die möglichen Mitigationsmaßnahmen und deren Limitierungen müssen tiefgehend verstanden werden. Das ist leider oft nicht der Fall – weder auf Anwenderseite noch in der Produktentwicklung. Viele Kunden und Lieferanten gehen davon aus, dass die gekauften Produkte und Komponenten ausreichend sicher sind und sie abgesehen von gelegentlichen Softwareupdates nichts weiter unternehmen müssen.

Echte Fortschritte lassen sich nur erzielen, wenn Politik, Hersteller und Anwender ein gemeinsames Grundverständnis der Risiken entwickeln. Hersteller sollten eine entsprechende Sicherheitskultur etablieren – ein langfristiger Prozess, der sich aber für alle Beteiligten auszahlt. Das funktioniert am besten in einem Markt, in dem auch die Anwender ein entsprechendes Problembewusstsein haben. Darüber hinaus muss die Politik Regeln festlegen, die eine bereits beim Markteintritt robuste Produktqualität fordern und fördern.

3. Security by Design in der Produktentwicklung

Security by Design für die Entwicklung sicherer Softwaresysteme umfasst mehrere Aspekte.

Hersteller müssen
- Schwachstellen proaktiv vermeiden, z. B. indem sie Komplexität reduzieren,
- sichere Entwicklungsmethoden nutzen und
- Sicherheit auch für ihre Supply Chain durchsetzen.

Eine vollständige Vermeidung von Fehlern ist aber nicht effizient möglich. Damit diese nicht zu ausnutzbaren Schwachstellen führen, braucht es eine mehrschichtige Sicherheitsarchitektur, welche Fehler antizipiert und mitigiert. Dazu gehört, nur wirklich benötigte Daten zu verarbeiten, gründliche Überprüfung von Eingangsdaten als auch Codeausführung in restriktiven Umgebungen.

Ein weiterer Aspekt betrifft die Komplexität. Sie lässt sich verringern, indem Anbieter den Funktionsumfang gezielt reduzieren und Funktionen modularisieren: Anwendungen werden in eigenständige Funktionseinheiten aufgeteilt, die über minimale, klar dokumentierte und restriktiv durchgesetzte Schnittstellen interagieren. Die hier übergebenen Daten kontinuierlich oder wiederkehrend zu überprüfen, ist dabei eine wichtige Ebene der mehrschichtigen Sicherheitsarchitektur und hilft, Fehler robust abzufangen. Die Software lässt sich zudem besser warten und der Einsatz von KI für Entwicklung, Review und Schwachstellenanalyse wird vereinfacht.

Module mit verschiedenen Aufgaben können Restriktionen in der Ausführungsumgebung unterworfen werden. Nicht jede Rechenoperation benötigt beispielsweise einen Zugriff auf das Netzwerk und den Massenspeicher. Eine solche Partitionierung von Anwendungen nach notwendigen Zugriffsrechten bietet eine weitere Sicherheitsschicht. Viele E-Mail- und SSH-Server und auch aktuelle Webbrowser basieren auf solchen Architekturen.

Doch damit nicht genug: Sichere Entwicklungsmethoden schließen weitere Aspekte ein. So sollten Programmiersprachen und Frameworks Fehler auf konzeptionelle Weise reduzieren oder vermeiden.

Beispiele dafür sind:
- moderne „Memory-Safe“-Programmiersprachen, die klassische Fehler bei der Speicherbehandlung ausschließen,
- Webframeworks, die ohne explizites Eingreifen der Entwickler gegen Cross-Site-Angriffe wie XSS und CSRF schützen oder durch mächtige Typisierung der Daten die Eingabeprüfung deutlich vereinfachen,
- Vorgehensweisen wie „Prepared Statements“, die Angriffsklassen wie SQL-Injection mitigieren und
- Bibliotheken und Werkzeuge, die zur Expertise der Entwickler passen und die keine speziellen Anpassungen benötigen, um sicher zu sein.

Durch die Anwendung von „Secure by Default“ in den Entwicklungsmethoden wird die Produktsicherheit implizit gesteigert, da Fehlbedienungen der Entwickler deutlich unwahrscheinlicher werden. Ein Beispiel sind die Bibliotheken im Bereich von Kryptografie und verschlüsselter Kommunikation (TLS). Sie waren in der Vergangenheit zwar sehr flexibel, erforderten jedoch von Entwicklern eine hohe Expertise und einen hohen Aufwand für eine sichere Nutzung. Das führt häufig zu kritischen Schwachstellen, da Programmierer unsichere Verschlüsselungsmethoden nutzen und Zertifikate fehlerhaft oder gar nicht prüfen.

Auch der Versuch, Entwicklern möglichst komfortable Entwicklungswerkzeuge zu schaffen, führt nicht selten zu unsicherem Verhalten. Ein wiederkehrendes Beispiel dafür ist die in vielen Programmiersprachen eingebaute Datenserialisierung. Sie ist sehr einfach und transparent nutzbar, birgt aber ein für den Programmierer nicht offensichtliches hohes Schadenspotenzial bei der Deserialisierung von Daten aus externen Quellen.

Ein weiterer Aspekt betrifft Open-Source-Komponenten: Die meisten Produkte werden nicht mehr komplett neu entwickelt, sondern nutzen extern entwickelte und gepflegte Programme, Bibliotheken und Ausführungsumgebungen. Open Source genießt zwar einen Vertrauensvorteil, da man den Quellcode prinzipiell begutachten und bei Bedarf anpassen kann. Das bedeutet jedoch weder, dass Experten tatsächlich eine Sicherheitsanalyse vorgenommen haben, noch dass die Qualität des Open-Source-Codes per se besser ist.

Security by Design bedeutet nicht zuletzt, die eigene Supply Chain im Griff zu haben. Eingesetzte Drittkomponenten müssen anhand ihrer Qualität bewertet und ausgewählt und wo nötig selbst verbessert werden. Gerade komplexe, aber essenzielle Anwendungen besitzen häufig eine lange Historie an Sicherheitslücken – und mit weiteren Schwachstellen in der Zukunft ist zu rechnen.
In der Konsequenz kann bei fremdentwickelten Komponenten – noch mehr als bei selbstentwickelten – eine restriktive Kapselung nötig sein, um die Auswirkung von Schwachstellen oder gar Backdoors robust zu begrenzen. Das führt am Ende zu stabileren und sicheren Produkten, weniger Nacharbeit und zufriedeneren Kunden.

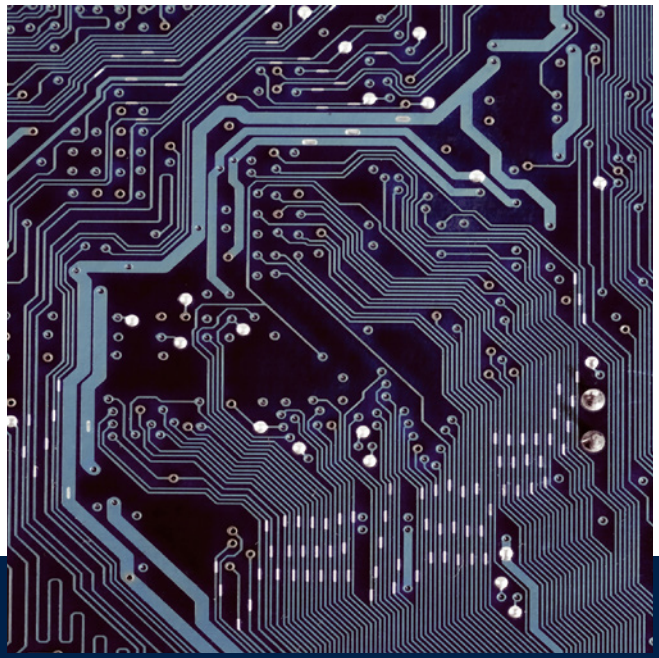
„Zertifikate und Zulassungen, die auf einer Prüfung durch vertrauenswürdige Stellen basieren, sind eine bessere Grundlage als die Versprechen der Hersteller.“

4. Security by Design in der Standardisierung

Komplexität und vielfach unnötige Flexibilität findet man leider auch bei Standards. Die Gremien versuchen Wünsche und Ideen aller Beteiligten und alle möglichen Anwendungsfälle zu berücksichtigen. Sicherheit spielt häufig nur eine untergeordnete Rolle – was auch für die Umsetzung dieser Standards in Systemen, Anwendungen und Bibliotheken gilt.

Das öffnet Tür und Tor für viele Angriffsvektoren: Daten können unterschiedlich interpretiert werden und so als Schwachstelle ausgenutzt werden. Oder präparierte Daten triggern direkt Sicherheitslücken in den Implementationen. Vermeintlich harmlose Umstände, wie die Vielfalt und Komplexität von Medienformaten für Bilder oder Videos, stellten sich in der Vergangenheit als erfolgreich genutzte Angriffsvektoren heraus.

Security by Design bedeutet in diesem Kontext, Standards möglichst restriktiv zu implementieren, ungewöhnliche oder fehlerhafte Eingabedaten explizit zu erwarten und die Implementation dagegen zu härten. Hier müssen alle an der Standardisierung Beteiligten ein Bewusstsein aufbauen.



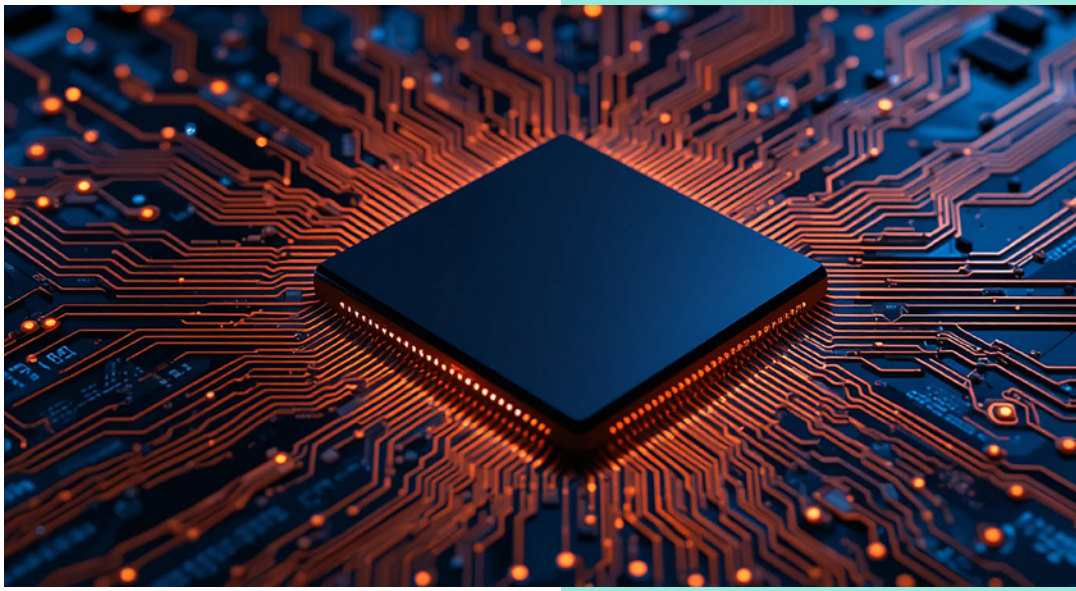
„Je genauer und restriktiver Parameter bei der Übergabe an den Schnittstellen zwischen einzelnen Funktionseinheiten geprüft werden, desto besser.“

5. Security by Design für Infrastrukturen

Security by Design wird primär für die Produktentwicklung propagiert. Ähnliche Herangehensweisen eignen sich jedoch für den Aufbau von Infrastrukturen. Besonders wichtig ist hier die Partitionierung nach Zugriffsrechten. Bereiche sollten segmentiert oder gar mikrosegmentiert werden und Mikroperimeter auf Netzebene geschaffen werden. Vorgeschaltete Zugriffskontrollen auf Anwendungsebene erlauben eine noch granularere Durchsetzung von Sicherheitsregeln. Diese granulare Beschränkung und Kontrolle von Zugriffen ist ein wichtiger Teil des Zero-Trust-Paradigmas.

Im Fokus steht hier die Güte der Authentisierung, die Sicherheit des zugreifenden Gerätes und der Abgleich weiterer Kontext-Parameter wie der Standort des Zugreifenden und sein bisheriges Verhalten. In gleicher Weise müssen die Parameter an den Schnittstellen zwischen den einzelnen Funktionseinheiten in einer Software überprüft werden – je genauer und restriktiver, desto sicherer.

Noch mehr Augenmerk verlangen Komponenten wie das Netzwerkmanagement, die Firewalls oder andere Sicherheitsprodukte: Diese können aufgrund ihrer Funktion in der Regel nicht oder schlecht limitiert werden. Hier muss verstärkt bereits beim Einkauf auf die Sicherheit geachtet werden. Zertifikate und Zulassungen, die auf einer Prüfung durch vertrauenswürdige Stellen basieren, sind eine solidere Grundlage als die Versprechungen der Hersteller. Mit einem Bündel von Maßnahmen lässt sich so auch die Infrastruktur sicherer gestalten.



6. Fazit

In dynamischen Märkten mit nicht klar definierten Rahmenbedingungen ist es eher die Regel als die Ausnahme, dass Hersteller unausgereifte Produkte auf den Markt bringen und diese nachbessern. Um aber einen für alle fairen Wettbewerb zu ermöglichen, der nicht zu Lasten von Anwendern und Gesellschaften geht, braucht es, ähnlich wie bei Lebensmitteln, Pharmaprodukten oder im Bauwesen, für alle Marktteilnehmer geltende Regularien sowie eine Lieferantenhaftung, die diese zu ausreichender Sicherheit verpflichtet.

Die Migration der Produktentwicklung hin zu einem Security by Design ist ein langjähriger und kostenintensiver Prozess. Es müssen firmenweit das Mindset geändert, hohe technische Expertise aufgebaut, Entwicklungsprozesse angepasst und vorhandener Legacy-Code inklusive der Supply-Chain gehärtet bzw. ersetzt werden.

Ein Aufwand, der sich auszahlt: Gut umgesetztes Security by Design und Security by Default bietet Anwendern und Lieferanten klare Vorteile. Kritische Softwareupdates werden seltener, Störungen im Betrieb nehmen ab und es gibt weniger hektische Bugfixes beim Lieferanten. Wenn die Komplexität sinkt, vereinfacht sich der Wartungsaufwand und die Lebensdauer der Produkte steigt – davon profitieren sowohl Lieferanten als auch Kunden.

Steffen Ullrich
Technology Fellow, genua GmbH

„genua ist direkt in die Entwicklung von OpenBSD involviert. Die resultierende In-House-Expertise ist eine wichtige Grundlage für Security by Design.“

7. Beispiel genugate Highly Resistant Firewall

Die Firewall genugate ist bereits früh auf hohe Sicherheitsbedürfnisse zugeschnitten worden und war 2002 das erste Produkt, das vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifiziert wurde. Inzwischen wird sie regelmäßig zertifiziert sowie für VS-NfD und vergleichbare Einstufungen im NATO und EU-Umfeld zugelassen. Ein besonderes Augenmerk gilt der hohen Widerstandsfähigkeit gegen Angriffe auf die Firewall selbst (CC EAL4+ AVA_VAN.5). Dies ist wichtig, da Firewalls an kritischen Netzübergängen stehen und oft auch Einblick in verschlüsselte Daten haben. Eine erfolgreiche Kompromittierung der Firewall würde einem Angreifer somit Zugriff auf das zu schützende Netz ermöglichen und eventuell auch Einblick in über die Firewall verschlüsselt transportierte Daten geben.

Zum hohen Selbstschutz trägt OpenBSD bei: Das Betriebssystem ist die Grundlage der genugate und anderer genua-Produkte. Es ist deutlich weniger komplex als andere Betriebssysteme wie Linux oder Windows. genua-Expertinnen und -Experten härten das Betriebssystem zusätzlich, indem sie beispielsweise Funktionen entfernen, die für den Betrieb als Firewall nicht nötig oder gar unerwünscht sind – ein Beispiel für angewendetes Security by Design.

Darüber hinaus laufen alle Prozesse, die externe und damit nicht vertrauenswürdige Daten verarbeiten, mit reduzierten Rechten und in restriktiven Umgebungen innerhalb des Systems – also quasi in einer Sandbox. Dadurch ist das System geschützt, selbst wenn es Schwachstellen bei der Datenverarbeitung geben sollte.

Noch restriktiver werden Virenscanner behandelt, die als binäre Drittprodukte außerhalb der genua-Kontrolle liegen, jedoch Zugriff auf sensitive Daten zur Analyse bekommen müssen. Diese Drittprodukte werden in eigenen virtuellen Maschinen ausgeführt und können keine Datenverbindung nach außen aufbauen. Selbst ein kritischer Fehler in dieser „eingesperrten“ Komponente kann daher nicht zu einer Exfiltration sensibler Daten führen.

„Wir verstehen tief im Design verankerte Sicherheit als wertvollen Mehrwert für unsere Produkte.“

Weitere Informationen:

genua.de/security-by-design

0925-01-DE

Über genua

Die genua GmbH mit Sitz in Kirchheim bei München sichert sensitive IT-Netzwerke im Public- und im Enterprise-Sektor, bei KRITIS-Organisationen und in der geheimschutzbetreuten Industrie mit hochsicheren und skalierbaren Cyber-Security-Lösungen. Dabei fokussiert sich das Unternehmen auf den umfassenden Schutz von Netzwerken, Kommunikation und interne Netzwerksicherheit für IT und OT. Das Lösungsspektrum umfasst Firewalls und Gateways, Virtual Private Networks, Fernwartungssysteme, interne Netzwerksicherheit und Cloud Security bis hin zu Remote-Access-Lösungen für mobiles Arbeiten und Homeoffice.

Die genua GmbH ist ein Unternehmen der Bundesdruckerei-Gruppe. Mit mehr als 400 Mitarbeitern entwickelt und produziert sie IT-Security-Lösungen ausschließlich in Deutschland. Seit der Unternehmensgründung 1992 belegen regelmäßige Zertifizierungen und Zulassungen durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) den hohen Sicherheits- und Qualitätsanspruch der Produkte. Zu den Kunden zählen u. a. Arvato Systems, BMW, die Bundeswehr, das THW sowie die Würth-Gruppe.

Teil der Bundesdruckerei-Gruppe

genua GmbH

Domagkstraße 7 | 85551 Kirchheim bei München
+49 89 991950-0 | info@genua.de | www.genua.de