WHITEPAPER

Secure by Design: Cybersecurity als Fundament

Warum diese Philosophie wichtig ist und wie sie Ihre Angriffsfläche von innen reduziert

SOPHOS

Kurzfassung

„Secure by Design“ ist eine Software-Entwicklungsphilosophie, die Sicherheit als grundlegende Anforderung betrachtet.

Anstatt zuerst ein Produkt zu entwickeln und Sicherheitskorrekturen erst später nachzurüsten, verlangt Secure by Design, dass Sicherheitsüberlegungen in jede Phase des Entwicklungslebenszyklus einfließen – von Architektur und Design über Codierung, Tests, Bereitstellung und Wartung.

Die Kernidee ist einfach: Wenn sichere Prinzipien von Grund auf integriert werden, sind Ihre Benutzer standardmäßig geschützt und nicht nur dann, wenn die richtigen Einstellungen konfiguriert sind oder Sicherheitslücken nachträglich geschlossen werden.

In der Praxis bedeutet das, Prinzipien wie „Least Privilege“ (Benutzer und Prozesse erhalten nur den minimalen Zugriff, den sie benötigen), sichere Standardeinstellungen (Auslieferung von Produkten mit der sichersten Konfiguration, die sofort einsatzbereit sind) und ganzheitliche Abwehrmaßnahmen (Schichtung mehrerer Sicherheitskontrollen, damit kein einzelner Fehler fatale Folgen haben kann) zu implementieren und durch sicherere Sprachen, Frameworks und Designmuster ganze Kategorien von Schwachstellen zu beseitigen.

Die Kernidee ist einfach:

Wenn sichere Prinzipien von Grund auf integriert werden, sind Ihre Benutzer standardmäßig geschützt und nicht nur dann, wenn die richtigen Einstellungen aktiviert sind oder Sicherheitslücken nachträglich geschlossen werden.

Warum wurde „Secure by Design“ eingeführt?

Jahrzehntelang wurde in der Technologiebranche vor allem nach dem Modell „Erst schnell auf den Markt bringen und später nachbessern“-Modell gearbeitet. Eine Folge davon ist, dass Cybersecurity von vielen als reiner Kostenfaktor betrachtet wird, der Releases verlangsamt und Entwickler frustriert. Die Auswirkungen spielen sich in Echtzeit ab: ständige Offenlegung von Schwachstellen, überstürzte Notfall-Patches und Sicherheitsverletzungen, die Unternehmen Milliarden kosten und gleichzeitig die personenbezogenen Daten von Hunderten Millionen Menschen offenlegen.

Die Ivanti Connect Secure-Schwachstellen, der Log4Shell Exploit in einer verbreiteten Open-Source Library und die MOVEit Transfer-Schwachstellen haben gezeigt, dass reaktive Sicherheit mit fest entschlossenen Angreifern einfach nicht Schritt halten kann.

Angesichts dieses Ungleichgewichts veröffentlichte die US-Behörde für Cybersicherheit und Infrastruktursicherheit (CISA) gemeinsam mit internationalen Partnern im Jahr 2023 offizielle Leitlinien zum Thema

„Secure by Design“ und forderte Technologiehersteller nachdrücklich auf, Verantwortung für die Sicherheitsergebnisse ihrer Kunden zu übernehmen.

Die „Secure by Design“-Prinzipien besagen, dass die Verantwortung für die Sicherheit bei den Herstellern liegen sollte, die die Produkte entwickeln, und nicht bei den Endnutzern, die sie einsetzen. Dieser Paradigmenwechsel hat den Sicherheitsfokus von Technologie-Anbietern von Eigenverantwortung („Benutzer sollten umgehend Patches einspielen“) auf Herstellerverantwortung („Anbieter sollten Produkte liefern, die vom ersten Tag an sicher sind“) verlagert.

Warum „Secure by Design“ für Cybersecurity-Lösungen von besonderer Bedeutung ist

Die Gefahr, dass Sicherheitstools selbst zum Einfallstor für Angriffe werden können, wird deutlich unterschätzt. Tatsächlich geschieht dies mit alarmierender Regelmäßigkeit.

Hierdurch offenbart sich eine kritische Schwachstelle für viele Unternehmen: Sobald ein Perimeter-Gerät exponiert wurde, kehren Angreifer wiederholt zu ihm zurück, bis der Schutz wieder vollständig aktiv ist. Firewalls und andere Edge-Systeme können anfällig bleiben, auch wenn ein Fix verfügbar ist. Laut einer aktuellen Analyse von Vorfällen, die von Sophos behoben wurden, vergehen von dem Moment, an dem ein Anbieter eine Empfehlung oder einen Patch veröffentlicht, bis zum Zeitpunkt, an dem ein Angreifer die Schwachstelle ausnutzt, durchschnittlich 322 Tage. Angreifer haben also fast ein ganzes Jahr Gelegenheit, Schwachstellen auszunutzen. Cybersecurity-Anbieter können nicht davon ausgehen, dass Benutzer Patches sofort installieren.

Das Problem der privilegierten Position

Cybersecurity-Tools nehmen die sensibelsten Bereiche der Infrastruktur eines Unternehmens ein. Endpoint Detection Agents werden mit Zugriff auf Kernelebene ausgeführt. SIEM-Plattformen erfassen Protokolle von jedem System. Identitätsanbieter besitzen die Schlüssel für jeden Account. Firewalls befinden sich an der Grenze zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken.

Wenn Sicherheitsprodukte das Herzstück der Abwehr eines Unternehmens bilden, tragen sie eine erhöhte Verantwortung für die Einhaltung der „Secure by Design“-Prinzipien. Anbieter in unserer Branche spielen eine entscheidende Rolle beim Schutz von Kunden, und dieses Vertrauen geht mit Erwartungen an die Art und Weise einher, wie Produkte entwickelt werden.

Diese privilegierte Position bedeutet, dass eine Schwachstelle in einem Sicherheitsprodukt nicht nur das Produkt selbst gefährdet, sondern auch alles, was es schützen soll. Ein Angreifer, der einen EDR (Endpoint Detection and Response) Agent kompromittiert, besitzt nicht nur ein einziges Tool, sondern auch den Endpoint mit den höchsten Berechtigungen. Eine Schwachstelle in einer VPN Appliance unterbricht nicht nur den Remote-Zugriff, sondern verschafft einem Angreifer einen direkten Zugang, der alle Perimeterkontrollen umgeht.

Was passiert, wenn „Secure by Design“ ignoriert wird?

Die Folgen einer Vernachlässigung der „Secure by Design-Prinzipien sind hinreichend dokumentiert und führen dazu, dass Unternehmen, Benutzer und das Internet insgesamt an Sicherheit einbüßen.

- **Eskalierende Kosten:** Werden Schwachstellen nach dem Release, also nach der Veröffentlichung entdeckt, ist die Behebung dieser Schwachstellen viel teurer als die Behebung während der Entwicklung.

- **Vertrauensverlust:** Kunden, Aufsichtsbehörden und Partner verlieren das Vertrauen in Unternehmen, die wiederholt von Sicherheitsvorfällen betroffen sind. Reputationsschäden können sich auch noch viele Jahre nach der technischen Bereinigung bemerkbar machen.

- **Regulative und rechtliche Risiken:** Regierungen weltweit verschärfen die Cybersecurity-Vorschriften. Der Cyber Resilienz Act der Europäischen Union schreibt beispielsweise verbindliche Sicherheitsanforderungen für Produkte mit digitalen Komponenten vor, die in Europa verkauft werden. Unternehmen, die die „Secure by Design“-Prinzipien missachten, riskieren Verstöße, Geldstrafen und den Ausschluss vom Markt.

- **Nationale Sicherheitsrisiken:** Kritische Infrastrukturen wie Stromnetze, Wasseraufbereitungsanlagen und Gesundheitssysteme sind zunehmend auf mit dem Internet verbundene Geräte und Systeme angewiesen. Unsichere Standardprodukte in diesen Umgebungen bieten staatlich finanzierten Angreifern und Ransomware-Betreibern Angriffsflächen – mit potenziell gravierenden Folgen für den Alltag vieler Menschen.

- **Patch-Müdigkeit:** Ohne sichere Grundlagen sind Unternehmen in einer reaktiven Schleife gefangen: Wiederholtes Scannen auf Schwachstellen, Priorisieren von Patches, Testen von Updates und Bereitstellen von Fixes. Dadurch werden Ressourcen gebunden, die für eingehendere Cybersecurity-Analysen genutzt werden könnten.

So finden Sie eine „Secure by Design“-Firewall

Bei der Wahl Ihrer nächsten Firewall sollte „Secure by Design“ oberste Priorität haben. Es kann jedoch schwierig sein, die Marketing-Botschaften der Anbieter zu durchschauen und zu verstehen, welche Funktionen eine Lösung tatsächlich bietet. Die folgenden Kriterien helfen Ihnen, die wichtigsten Merkmale zu identifizieren, auf die Sie bei der Auswahl einer Firewall achten sollten, die auf echten „Secure by Design“-Prinzipien basiert:

1. Gehärtete Architektur

Wie wir gesehen haben, ist es von entscheidender Bedeutung, dass die Architektur der Firewall vom Code bis zum Kern auf „Secure by Design“ ausgelegt ist. Aber wie können Sie sichergehen, was ein bestimmter Firewall-Anbieter wirklich getan hat, um sein Produkt zu härten? Die meisten Anbieter behaupten zwar, ihre Produkte seien sicher, doch letztendlich wird ihre jüngste Erfolgsbilanz die Wahrheit ans Licht bringen.

Hier sind einige offensichtliche Punkte, die Sie überprüfen sollten:

- Unterstützung von Multi-Faktor-Authentifizierung (MFA) in allen Firewall-Bereichen (Admin, VPN, Portale).
- Integrierte Unterstützung von Zero Trust Network Access (ZTNA), sodass kein Remote Access VPN mehr erforderlich ist
- Sichere Remote-Verwaltung, die KEIN SSH oder KEINEN Remote-Login über das Internet erfordert
- Gehärtete und containerisierte Benutzerportale, wenn diese mit dem Internet verbunden sind
- Aktuelle Versionsinfos des Anbieters, die darauf hinweisen, dass „Secure by Design“-Prinzipien erfüllt werden

2. Automatisches Patchen von Schwachstellen ohne Ausfallzeiten

Einer der größten Angriffsvektoren auf Netzwerkinfrastrukturen sind ungepatchte Schwachstellen. Nachdem eine Schwachstelle entdeckt wurde, kann es Wochen dauern, bis sie gepatcht wird. Viele Benutzer leiden unter sogenannter „Patch-Müdigkeit“, da sie ständig neue Patches installieren und die damit verbundenen Ausfallzeiten regelmäßig in Kauf nehmen müssen.

Entbinden Sie Ihre Benutzer von dieser lästigen Aufgabe und stellen Sie sicher, dass Ihre Systeme schnell gepatcht werden, indem Sie mit einem Anbieter zusammenarbeiten, der automatische Over-the-Air-Updates ohne Ausfallzeiten bietet. Fallen Sie nicht auf die Marketing-Versprechen sogenannter „automatischer Updates“ herein – prüfen Sie, was „automatisch“ wirklich bedeutet. Updates, die nach wie vor einen Neustart und Ausfallzeiten erfordern, sind nicht „automatisch“.

3. Automatische Überwachung des Konfigurationsrisikos

Eine weitere häufige Ursache von Sicherheitsvorfällen sind Fehlkonfigurationen der Firewall. Leider melden die meisten Firewalls nicht selbst, dass sie falsch konfiguriert sind, wodurch viele Sicherheitslücken unentdeckt bleiben. Ihre nächste Firewall sollte daher in der Lage sein, wichtige Konfigurationen automatisch und kontinuierlich zu überprüfen und hochriskante Einstellungen zu melden, damit Sie diese einfach beheben können.

4. Proaktives Monitoring durch den Anbieter

Bei den meisten Firewalls erfahren Sie erst zu spät, dass diese angriffen wurden. Glücklicherweise ist dies nicht bei jeder Firewall der Fall. Wählen Sie einen Firewall-Anbieter aus, der seine eigenen Produkte remote überwacht und Telemetriedaten sammelt, um Anzeichen einer Kompromittierung frühzeitig zu erkennen. Anbieter sollten bereit und in der Lage sein, schnell zu reagieren, wenn ungewöhnliche Aktivitäten erkannt werden, indem sie sich schnell an Sie oder Ihren Cybersecurity-Partner wenden, um den Angriff zu identifizieren und zu beheben.

5. Ein Anbieter, der sich zu „Secure by Design“ verpflichtet

Wenn Sie bis hierher gekommen sind, haben Sie wahrscheinlich bereits einen Anbieter im Auge, der sich klar den „Secure by Design“-

Prinzipien verschrieben hat. Aber vertrauen Sie den Versprechungen des Anbieters nicht blind. Informieren Sie sich über die jüngste Entwicklung, Fortschrittsberichte und Versionsinfos des Anbieters, um genau zu verstehen, wie sehr sich das Unternehmen für Ihre Sicherheit einsetzt.

Takeaways

„Secure by Design“ steht im Einklang mit unseren zentralen Unternehmenswerten im Bereich Transparenz und ist eine führende Kraft bei der kontinuierlichen Bewertung und Verbesserung unserer Sicherheitspraktiken.

Sophos‘ Engagement für Secure by Design

Am 8. Mai 2024 hat sich Sophos sich als eines der ersten Unternehmen der Initiative „Secure by Design“ der US-Behörde für Cybersicherheit und Infrastruktursicherheit (CISA) angeschlossen, die sich auf sieben Kernsäulen der Technologie- und Produktsicherheit konzentriert:

1. Multi-Faktor-Authentifizierung
2. Standardpasswörter
3. Reduzierung ganzer Schwachstellen-Kategorien
4. Sicherheitspatches
5. Richtlinie zur Offenlegung von Schwachstellen
6. CVEs
7. Kompromittierungs-Indizien

Im Einklang mit unseren zentralen Unternehmenswerten im Bereich Transparenz ist „Secure by Design“ eine treibende Kraft bei der kontinuierlichen Bewertung und Verbesserung unserer Sicherheitspraktiken.

Wir haben unsere Eigenverpflichtungen zur Verbesserung unserer Praktiken veröffentlicht und berichten regelmäßig über die Fortschritte, die wir in Bezug auf die sieben Kernsäulen des „Secure by Design“-Frameworks erzielen. Natürlich entwickelt sich die Cybersicherheit ständig weiter und diese Aufgabe ist nie „erledigt“. Die kontinuierliche Weiterentwicklung und Verbesserung der Anwendung der „Secure by Design“-Prinzipien in unserem gesamten Portfolio ist ein fester und zentraler Bestandteil unserer Unternehmensphilosophie.

Sophos bietet eine Reihe wichtiger „Secure by Design“-Funktionen, die den Sicherheitsstatus der Sophos Firewall deutlich verbessern und Ihnen gleichzeitig viele Aufgaben abnehmen. Die Sophos Firewall bietet als marktweit einzige Firewall wirklich

automatische Over-the-Air-Sicherheitspatches, die keinerlei Ausfallzeiten erfordern. Außerdem überwachen wir als einziger Anbieter unsere gesamte Installationsbasis von Kunden-Firewalls aktiv auf Anzeichen von Angriffen, damit wir schnell reagieren können, um Ihnen und Ihrem Cybersecurity-Partner bei der Bereinigung zu helfen – und alle anderen Kunden sofort vor ähnlichen Angriffen zu schützen.

Die neueste Version (v22) der Sophos Firewall bietet noch mehr „Secure by Design"-Funktionen und verbessert den Sicherheitsstatus der Firewall erheblich. Zu diesen Funktionen gehören:

- Eine neue Heath-Check-Funktion, die das Risiko von Fehlkonfigurationen senkt, die zu Angriffen führen könnten
- Eine komplett neue Steuerungsebene, die für maximale Sicherheit und Skalierbarkeit neu konzipiert wurde und eine ganze Kategorie von Schwachstellen beseitigt
- Ein Sophos XDR Linux Sensor, der die Echtzeit-Überwachung der Systemintegrität unserer gesamten Kundenbasis durch unsere eigenen Sicherheitsteams verbessert, sodass diese Angriffe schneller erkennen und darauf reagieren können
- Firmware-Updates, die nun verschlüsselt und zur Gewährleistung der Echtheit mit einem Zertifikat versehen sind
- Upgrade auf die neueste Anti-Malware Engine von Sophos mit verbesserter Zero-Day-Echtzeit-Erkennung neuer Bedrohungen

Unsere Arbeit im Rahmen der Pacific-Rim-Kampagne gab uns einen ersten Einblick, wie entschlossen und gut ausgestattet Bedrohungsakteure agieren – und was es wirklich braucht, um sich vor ihnen zu schützen. Die Kampagne hat deutlich gemacht, dass Angreifer nicht darauf warten, dass Schwachstellen auftreten, sondern aktiv nach Design-Mängeln, Konfigurationslücken und ungepatchten Systemen in der gesamten globalen Infrastruktur suchen. Diese Erfahrung hat unser „Secure by Design"-Konzept direkt beeinflusst.

Moderne Sicherheitsmaßnahmen müssen damit beginnen, die Angriffsfläche auf Produktebene zu verringern, robuste Standardeinstellungen zu integrieren, Authentifizierungsprozesse zu verschärfen und Möglichkeiten für Missbrauch zu beseitigen, lange bevor eine Sicherheitslücke überhaupt in Umlauf gelangt.

Der Weg nach vorne

„Secure by Design" beseitigt nicht alle Schwachstellen und entbindet Unternehmen nicht von kontinuierlicher Wachsamkeit. „Secure by Design" ist jedoch zum grundlegenden Cybersecurity-Fundament geworden, um die Angriffsfläche zu reduzieren. Die Frage ist nicht mehr, ob „Secure by Design" eine gute Idee ist, sondern wie schnell dieses Konzept umgesetzt werden kann.

Bereit, Ihr Cybersicherheits-programm zu bewerten?

Sprechen Sie noch heute mit einem Sophos-Experten.

Sales DACH (Deutschland, Österreich, Schweiz)
Tel.: +49 611 58580
E-Mail: sales@sophos.de