Vom Code zum Kunden: So garantieren wir die Sicherheit unserer Produkte

kaspersky BRING ON THE FUTURE

www.kaspersky.de

Zusammenfassung

Je vernetzter die Welt wird, desto wichtiger ist sichere und vertrauenswürdige Technologie. Und auch die Sicherheit entsprechender Produkte selbst gewinnt immer mehr an Bedeutung. Sicherheitsprodukte entwickeln sich mit der Schwachstellenforschung weiter und je umfang-reicher die Bedrohungslandschaft wird, desto komplexer werden auch Struktur und Aufbau unserer Produkte.

Software-Entwicklung ist ein vielschichtiger Prozess mit vielen verschie-denen Phasen auf dem Weg vom Code zum Kunden. Im Gegensatz zur meisten anderen Software umfassen Sicherheitsprodukte zahlreiche Komponenten, von denen einige eng in das Betriebssystem integriert sind. Aus diesem Grund ist die Behebung von Sicherheitsproblemen unerlässlich, damit nicht das gesamte System ausfällt.

Eine der Herausforderungen in der Software-Entwicklung ist es, Situationen zu vermeiden, in denen dasselbe Problem immer und immer wieder auftritt. Denn ein solches Szenario ist wenig effizient und birgt viele Gefahren.

Wenn Architektur oder Softwarekomponenten richtig angegangen werden, lässt sich diese Situation vermeiden. Und in Kombination mit einem kollaborativen Lebenszyklus in der Software-Entwicklung, bei dem Sicherheit in jedem Schritt des Entwicklungsprozesses Priorität hat, werden die Produkte sogar noch sicherer. Und genau so geht Kaspersky vor: Wir verfolgen einen grundlegenden strategischen Ansatz, der teamübergreifende Zusammenarbeit, vielseitige interne und externe Informationsquellen sowie regelmäßige Schulungen umfasst.

Wir haben den gesamten Prozess weiterentwickelt und so eine Umgebung geschaffen, in der wir Sicherheit optimal in unsere Produkte integrieren können. Lesen Sie weiter, um mehr über unsere Vorgehensweise zu erfahren.

Vom Code zum Kunden: So garantieren wir die Sicherheit unserer Produkte

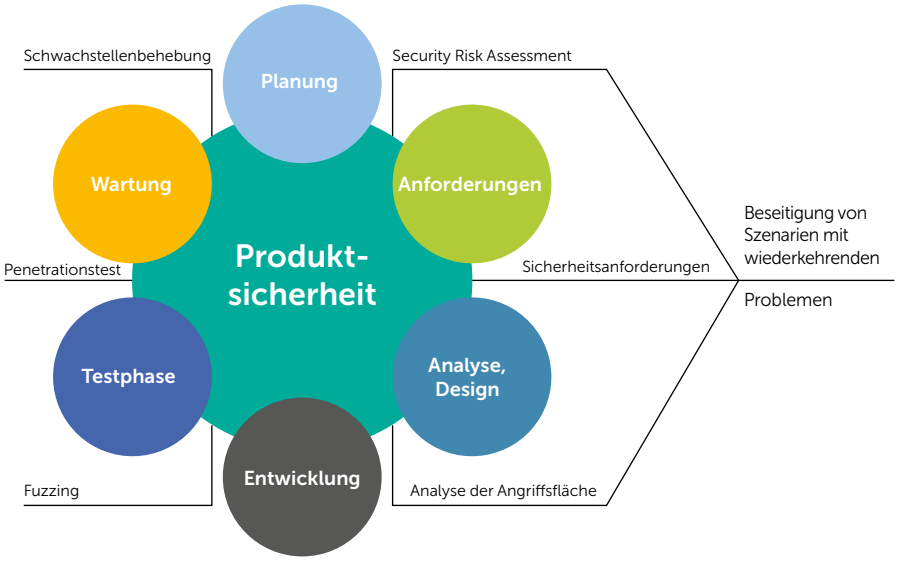
Bei Kaspersky nehmen wir unsere Rolle als einer der führenden Sicherheitsanbieter sehr ernst. Bei der Entwicklung unserer Produkte handeln wir bei jedem Schritt nach unseren Kernprinzipien für sichere Produkte. Im Gegensatz zu anderer Software umfassen Sicherheitsprodukte viele Komponenten, von denen einige eng ins Betriebssystem integriert sind, weshalb die Behebung von Sicherheitsproblemen in unseren Produkten so wichtig ist.

Über zwei Jahrzehnte ist es her, dass wir unsere erste Antivirenlösung entwickelt haben. Während dieser Zeit haben wir viel Erfahrung sammeln können, sodass wir heute genau wissen, wie wir schnell und effektiv auf neue Herausforderungen der Cybersicherheit reagieren können. Unsere Sicherheitsprodukte – und andere Software – entwickeln sich mit der wachsenden Branche der Schwachstellenforschung weiter. Und je umfangreicher die Bedrohungslandschaft wird, desto komplexer werden auch Struktur und Aufbau unserer Produkte – mit Verbesserungen und neuen Funktionen in jeder Version.

Wir kennen den direkten Zusammenhang zwischen Komplexität und der Anzahl potenzieller Schwachstellen, die sich im entsprechenden Produkt finden lassen. Unsere Spezialistenteams sowie unser gesamter Entwicklungsprozess sind darauf ausgerichtet, bei unseren Software-Engineering-Prozessen höchstmögliche Sicherheit zu gewährleisten. Denn bestmöglicher Schutz ist der Kern unserer Arbeit.

Entscheidend ist das Fundament

Wenn die Architektur von Softwarekomponenten richtig angegangen wird, lassen sich Szenarien, in denen Probleme wieder und wieder auftreten, vermeiden. Dasselbe gilt für die Behebung von Schwachstellen. Unsere Produktteams arbeiten eng mit dem Team für Produktsicherheit zusammen, um zu gewährleisten, dass unsere Architektur sicher ist.

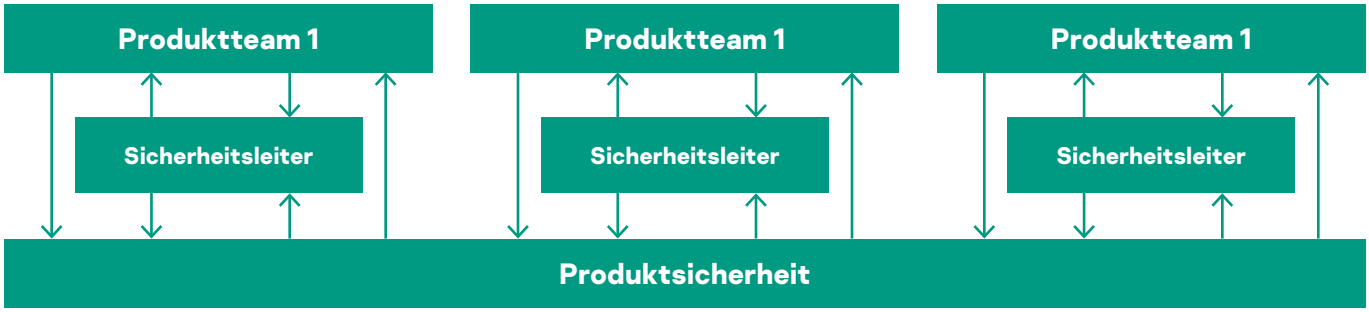


Sicherheit beim Entwicklungsprozess: Insbesondere durch die ersten drei Schritte – Planung, Anforderungen und Analyse sowie Design – lassen sich wiederkehrende Probleme vermeiden.

Mit diesem Ansatz konnten wir die Probleme vermeiden, die Parisa Tabriz, Sicherheitsexpertin bei Google, in ihrer Keynote bei der Black Hat USA 2018 beschrieben hat. In ihrer Rede besprach Tabriz ein Problem, das alle Entwickler kennen: wie frustrierend es ist, wenn Meldungen zu Sicherheitsschwachstellen eingehen, die eigentlich schon behoben wurden, wenn eine simple Variante eines bekannten Fehlers vorkommt oder wenn Symptome fehlgeschlagener Bedingungen oder Prozesse auftreten, die zwar bekannt sind, aber nicht behoben wurden.

Und genau hier setzt der sichere Entwicklungslebenszyklus von Kaspersky an, ein Ansatz, bei dem Sicherheit bei der Produktentwicklung oberste Priorität hat. Indem Szenarien mit wiederkehrenden Fehlern schon während der Architekturentwicklung vermieden werden, lassen sich auch spätere Probleme mit denselben Schwachstellen verhindern. Darüber hinaus werden so Ressourcen freigesetzt, die für die Entwicklung anderer Produkte oder die Unterstützung bereits veröffentlichter Produkte eingesetzt werden können. Das Ergebnis ist eine sichere Produktarchitektur, die zahlreiche Vorteile bietet:

- Minimierung von Schwachstellen, die bei der Wartungsphase der Entwicklung zu schwerwiegenden Architekturänderungen an Kernkomponenten führen können
- Freigesetzte Ressourcen bei der Wartungsphase
- Reduzierung erforderlicher Sicherheitsupdates



So interagieren die Produkt- und Sicherheitsteams: Der Sicherheitsleiter ist eine zusätzliche Ebene, die gewährleistet, dass Informationen vom Team für Produktsicherheit richtig angewendet werden.

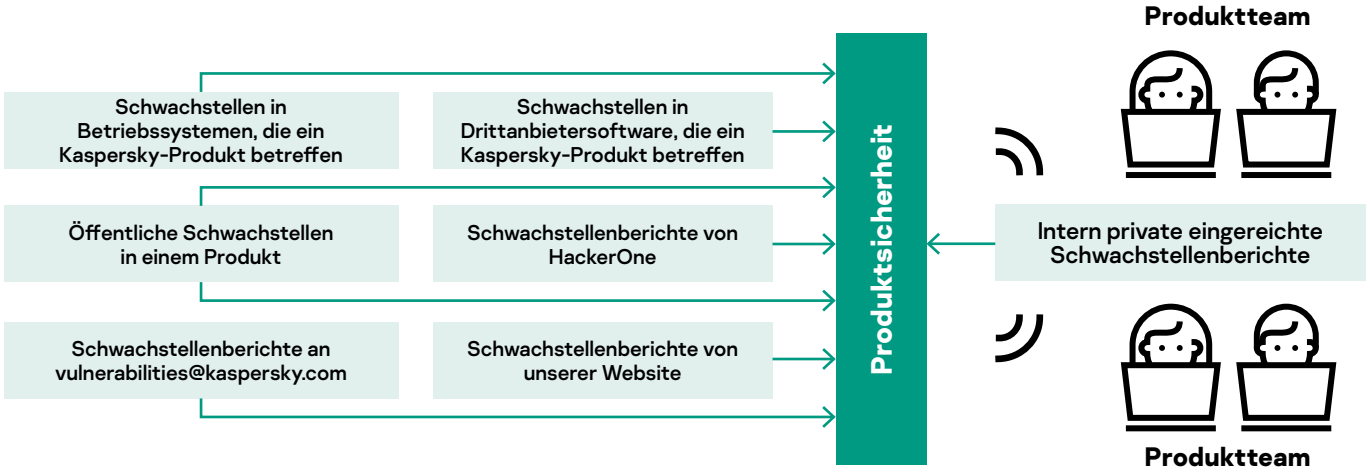
Unser Team für Produktsicherheit ist der Ausgangspunkt für die gesamte Forschung und Entwicklung hinsichtlich sämtlicher Sicherheitsprobleme von Produkten und Infrastruktur. Das Team übernimmt eine Reihe wichtiger Aufgaben, darunter die Vorbereitung der Grundanforderungen, Codeprüfungen, Schwachstellenbearbeitung, Risikoanalyse, Vulnerability Assessment, Bereitstellung von Behebungsmöglichkeiten, Integration von Fuzzing-Prozessen und Penetrationstests. Unser Forschungsteam für Malware-Schutz stellt während dieser Schritte wichtigen Input bereit.

Quellen für Schwachstelleninformationen

Selbst nachdem das Produktteam viel Zeit in das Schreiben des Softwarecodes gemäß Sicherheitsstandards investiert hat, können Angreifer Schwachstellen im Produkt oder in seiner Umgebung (dem Betriebssystem) finden und ausnutzen. Aus diesem Grund nutzen wir vielseitige Quellen für Schwachstelleninformationen, um unsere Produktsicherheit zu optimieren.

Folgende Quellen kommen hierbei zum Einsatz: offengelegte Schwachstellen in Betriebssystemen, die unsere Produkte betreffen könnten, Schwachstellen in Drittanbieter-Bibliotheken oder -Software, die wir in unseren Produkten verwenden, öffentliche Schwachstellenberichte von Forschungsteams, Berichte aus dem Portal unseres „Bug Bounty"-Programms (bei dem es Prämien für gefundene Schwachstellen gibt), Berichte, die Hacker an unser Schwachstellen-Postfach senden (vulnerabilities@kaspersky.com), Berichte, die Forscher über unser Onlineformular einreichen, sowie von unseren Forschern, Softwarearchitekten und Penetrationstestern privat gemeldete Schwachstellen.

Von Kaspersky genutzte Quellen für Schwachstelleninformationen

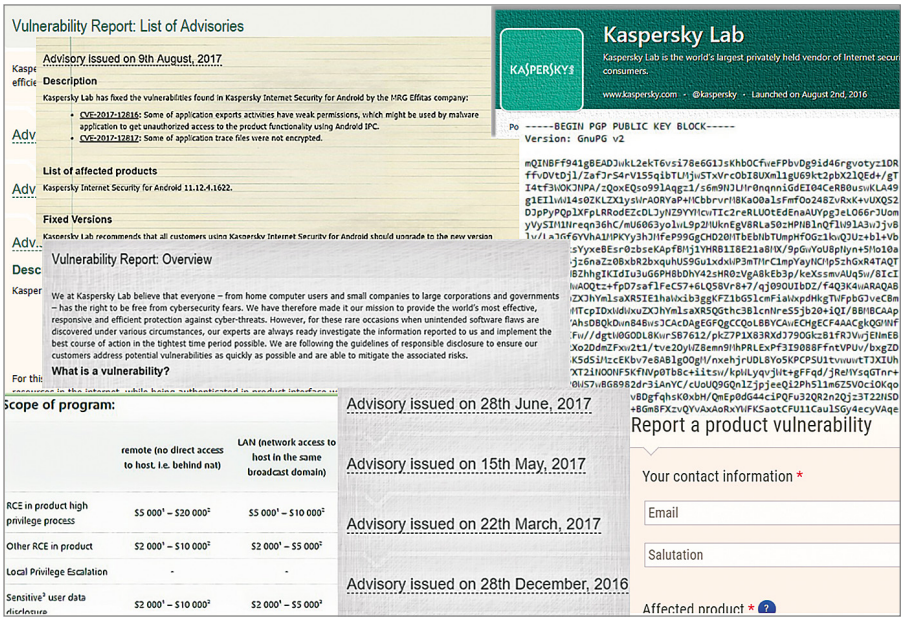


Offengelegte ungepatchte Schwachstellen in unseren Produkten sind kritisch, da Cyberkriminelle sie ausnutzen könnten, um unsere Kunden anzugreifen. Je nach CVSS-Bewertung (Common Vulnerability Scoring System) und potenziellen Auswirkungen auf Kunden hat die Behebung dieser Schwachstellen oberste Priorität. Auch die Behebung offengelegter Schwachstellen in Betriebssystemen und Drittanbietersoftware, die unsere Produkte betreffen, ist entscheidend.

Die **HackerOne-Plattform zum Melden von Schwachstellen** bietet uns eine flexible und geregelte Möglichkeit, Berichte von Forschern entgegenzunehmen. Der Plattform-Workflow für die Verarbeitung von Schwachstellenberichten beginnt mit der Sichtung eingesendeter Berichte, umfasst Prämien für gefundene Schwachstellen und behandelt die Offenlegung vertraulicher Informationen zu einer bestimmten Schwachstelle. (Hacker können nach Behebung oder öffentlicher Bekanntgabe des Problems eine vollständige oder teilweise Informationsoffenlegung zur entsprechenden Schwachstelle anfordern.)

Manche der Personen, die Schwachstellen melden, senden ihre Entdeckungen direkt an unser **spezielles Postfach zum Melden von Schwachstellen:** vulnerabilities@kaspersky.com. Wir empfehlen, beim Einreichen dieser vertraulichen Informationen die Verschlüsselung über unseren öffentlichen PGP-Schlüssel zu verwenden. Dieser wird in der Branche häufig zum Schutz entsprechender Prozesse eingesetzt.

Quellen für Schwachstellenberichte



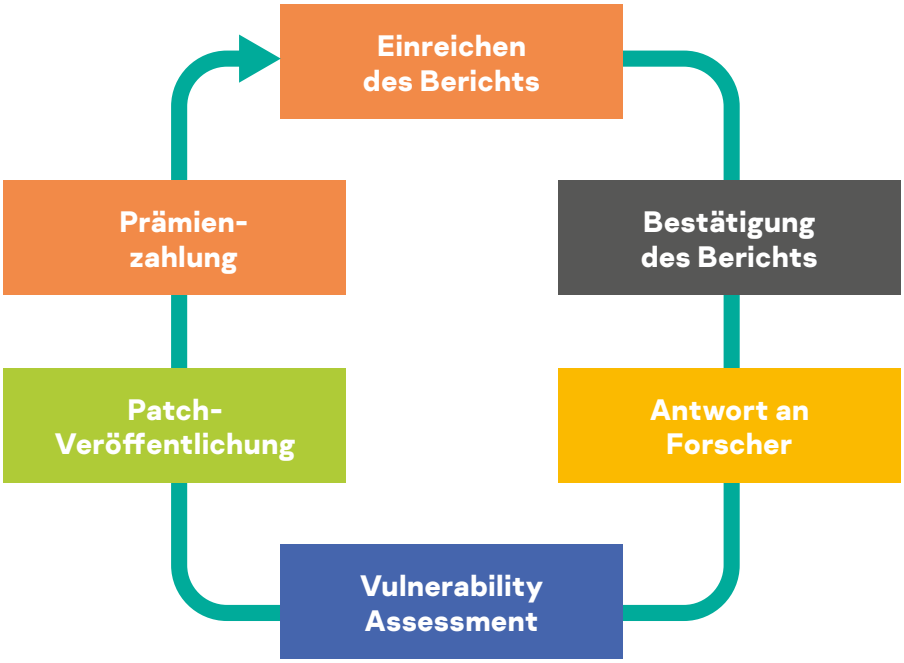
Reaktion auf Berichte

Die Reaktion auf Schwachstellenberichte ist ein separater Prozess mit einem speziellen Workflow. Dieser Prozess beginnt, wenn wir Informationen zu einer potenziellen Schwachstelle erhalten, die möglicherweise unsere Produkte betrifft. Manchmal erhalten wir Berichte zu vermeintlichen Schwachstellen in unseren Produkten, die jedoch letztlich Schwachstellen in einem Betriebssystem betreffen. Auch in diesen Fällen stellen wir ein Update bereit, um die Situation zu beheben.

Die Beteiligung von Kaspersky an dem „Bug Bounty"-Programm von HackerOne spiegelt die wachsenden Herausforderungen der Sicherheitsbranche wider. Natürlich beschäftigen wir auch interne und hoch spezialisierte Forscher und Lösungsarchitekten, doch externe unabhängige Sicherheitsforscher bringen individuelle Sicht- und Denkweisen mit sich. Und indem wir diesen externen Experten Penetrationstests unserer Produkte ermöglichen, können wir ihre Zuverlässigkeit und Sicherheit weiter steigern als nur mit internen Ressourcen.

Außerdem ist es unserer Meinung nach nicht nur sinnvoll, sondern sogar smart, Hacker für das Melden von Schwachstellen zu bezahlen – denn wenn das nicht passiert, kommen sie vielleicht auf die Idee, ihre Informationen stattdessen an Cyberkriminelle zu verkaufen. Ihre Berichte müssen strenge Richtlinien erfüllen, damit wir sie annehmen, darunter eine ausführliche Erklärung der gemeldeten Schwachstelle sowie technische Details und ein Beispiel eines zuverlässigen funktionierenden Exploits bzw. ein Wirksamkeitsnachweis.

Workflow zur Schwachstellenverarbeitung in einem „Bug Bounty“-Szenario



Der Umfang unseres „Bug Bounty“-Programms umfasst derzeit Kaspersky Internet Security 2019 Beta und Kaspersky Endpoint Security 11. Die Schwachstellen-Exploits müssen Windows-Versionen ab 8.1 betreffen und vergütet wird hierbei die Entdeckung von RCE- (Remote Code Execution, Remote-Codeausführung), LPE- (Local Privilege Escalation, Steigerung lokaler Berechtigungen) sowie ID-Schwachstellen (Information Disclosure, Informationsoffenlegung). Letztere sind auf vertrauliche Informationen wie Passwörter, Zahlungsdaten oder Authentifizierungs-Token beschränkt. Für einen ausführlichen Bericht und ein funktionierendes Beispiel der Schwachstelle <<unicorn>>, über die Angreifer auf dem MITM-Vektor (Man in the Middle) remote schädlichen Code in hochrangigen Prozessen ausführen können, kann die Prämie bis zu 100 000 US-Dollar betragen.

	Ring 3 (niedrige Berechtigungen)	Ring 3 (hohe Berechtigungen)	Ring 0	Ring -1
AV-Umgehung				
Information Disclosure (ID)				
Local Privilege Escalation (LPE)				
Remote Code Execution (RCE)				

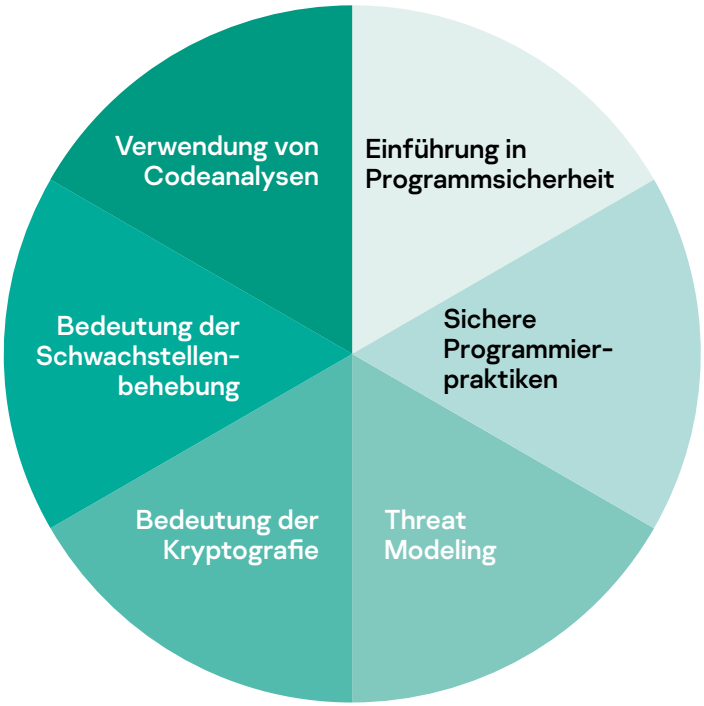
Arten der in Antivirenprodukten gefundenen Schwachstellen: Angreifer nutzen AV-Umgehungen, um große Teile des Schutzes eines Produkts zu umgehen. Je dunkler das Feld, desto schwerwiegender die Gefahr.

- Im Benutzermodus **(Ring 3)** werden Antivirendienst und GUI-Prozesse ausgeführt. Der Antivirendienst ist ein Prozess mit hoher, die GUI einer mit niedriger Priorität.
- Antivirentreiber werden im **Kernel-Modus** ausgeführt **(Ring 0)** und greifen auf den Windows-Kernel und alle Prozesse im virtuellen Arbeitsspeicher zu. Diese Art von Exploit ist äußerst gefährlich, da Ring 0 über die meisten Berechtigungen verfügen und eine erfolgreiche Ausnutzung dieser Berechtigungen das gesamte System beeinträchtigen kann.
- Manche Antivirenprodukte beinhalten spezielle Komponenten, die auf Hypervisorebene **(Ring -1)** arbeiten. Diese Komponenten steuern speicherübergreifende Vorgänge und bieten Schutz vor Screenshotting. Die Ausnutzung einer Schwachstelle auf dieser Ebene beeinträchtigt virtuelle Maschinen und kann auch integrierte Sicherheitsmaßnahmen, wie z. B. Microsoft Device Guard und Credential Guard, umgehen.

Man lernt nie aus

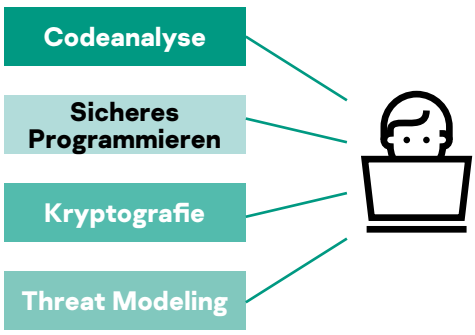
Mit der Integration sicherer Prozesse in unseren Entwicklungslebenszyklus halten wir auch unsere Entwickler und Architekten an, sich mit diesen Prozessen zu befassen. Wir kombinieren unser Wissen rund um die sichere Entwicklung unserer bisherigen F&E-Erfahrung mit Einblicken von unserem Team für Produktsicherheit, das seine Daten und Fertigkeiten ständig mit neuen Prozessen erweitert und aktualisiert. So können wir folgende wichtige Bereiche bei unseren Schulungen zu Produktsicherheit abdecken:

Sicherheitsschulung für Entwickler, Techniker und Architekten



Dieser Ansatz bietet unseren Entwicklern und dem gesamten Unternehmen viele Vorteile. Weitere Informationen hierzu finden Sie in der Abbildung unten. Der Ansatz motiviert nicht nur unsere Entwickler, sich auch mit anderen Bereichen der Computersicherheit zu befassen, sondern reduziert auch die Gesamtkosten für Softwarewartung und verbessert unseren Markenruf.

Vorteile laufender Entwicklerschulungen



Vorteile

- Geringere Ausgaben für Sicherheitsupdates
- Freigesetzte Ressourcen für Produktunterstützung
- Verbesserte Reputation des Unternehmens
- Verbesserte Entwicklerfertigkeiten

Sicherheit auf jedem Schritt

Der Prozess zur Entwicklung sicherer Software ist nicht leicht, insbesondere bei komplexen Produkten und Lösungen. Um optimale Sicherheit zu gewährleisten, muss sie in jeder Phase von Software-Entwicklung und Wartungsprozess Priorität haben. Dies beinhaltet das Zusammenstellen der Sicherheitsanforderungen, Risikobewertungen, Analysen der Angriffsfläche, Fuzzing, Penetrationstests, Schwachstellenbehebung und Entwicklerschulungen. Und das ist der Kern unserer Arbeit bei Kaspersky. Das Ergebnis? Die weltweit am meisten getesteten und ausgezeichneten Sicherheitslösungen.

Neues über Cyberbedrohungen: https://de.securelist.com
IT Security News: https://www.kaspersky.de/blog/b2b/
Cybersicherheit für KMUs: kaspersky.de/business
Cybersicherheit für Großunternehmen: kaspersky.de/enterprise

www.kaspersky.de

Beständigkeit, Unabhängigkeit und Transparenz – das zeichnet uns aus. Wir wollen eine sichere Umgebung schaffen, in der Technologie unser Leben verbessert. Deshalb schützen wir sie, damit Menschen auf der ganzen Welt die unzähligen technologischen Möglichkeiten nutzen können. Wir tragen mit Cybersicherheit zu einer sicheren Zukunft bei.

Erfahren Sie mehr unter kaspersky.com/transparency

Getestet.
Transparent.
Unabhängig.