.experience

Cybersecurity
Eine moderne Wildwest-Geschichte

Ein Magazin von ERNI seit 1999.

Editorial

Liebe Leserinnen und Leser,

Cybersicherheit wird oft im Zusammenhang mit Tools, Vorfällen und Vorschriften thematisiert. Hinter jedem sicheren oder unsicheren System stehen jedoch Menschen, die täglich Entscheidungen treffen.

In dieser Ausgabe von .experience betrachten wir Cybersicherheit aus einer anderen Perspektive und erzählen die Geschichte von drei Charakteren: «dem Guten, dem Hässlichen und dem Bösen». Das Gute entwickelt Software, bei der Sicherheit von Anfang an im Vordergrund steht. Das Hässliche sorgt für Compliance, Governance und Verantwortlichkeit in einem immer komplexer werdenden regulatorischen Umfeld. Das Böse hinterfragt Annahmen, indem es aktiv versucht, Systeme zu knacken, bevor echte Angreifer dies tun.

Diese Perspektiven werden in drei Referenzfällen zum Leben erweckt. Sie erfahren, wie sich bewährte Sicherheitsverfahren auf professionelle Entwicklungsteams übertragen lassen, wie Sicherheit über den gesamten Produktlebenszyklus hinweg gestaltet werden kann und wie Penetrationstests reale Angriffe aufdecken, die oft verborgen bleiben.

Wir laden Sie ein, sich auf eine aufschlussreiche Entdeckungsreise zu begeben und Inspiration zu finden, wie Sie diese Erkenntnisse in Ihren eigenen Teams anwenden können.

Herzliche Grüsse,

Pavo Kohler
CEO, ERNI Group

Inhalt

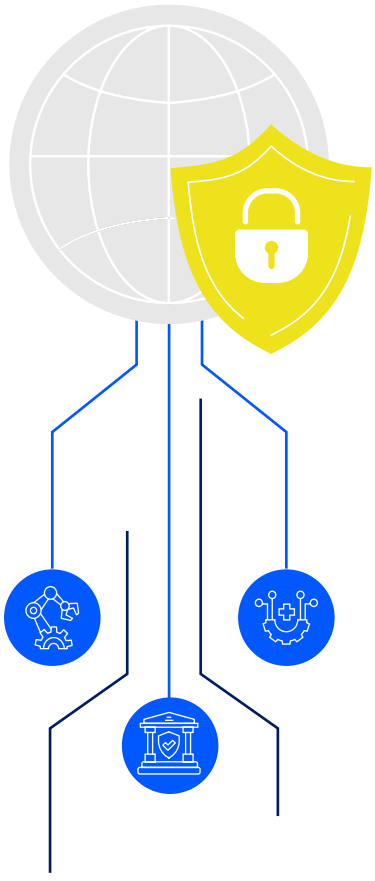
Cybersicherheit in Zeiten der Unsicherheit

In der vernetzten Welt ist Cybersicherheit längst kein reines IT-Thema mehr. Sie ist eine geschäftliche Notwendigkeit. Organisationen bewegen sich in einem Umfeld, das von schneller Digitalisierung, geopolitischen Spannungen, wirtschaftlicher Unsicherheit und sich ständig verändernden Bedrohungen geprägt ist. Software steuert kritische Dienstleistungen, Daten bilden die Grundlage für businessrelevante Entscheidungen, jede digitale Verbindung ist Chance und Risiko zugleich.

Von Albert Alsina, Geschäftsführer, ERNI Spanien

Wie stark einzelne Branchen betroffen sind

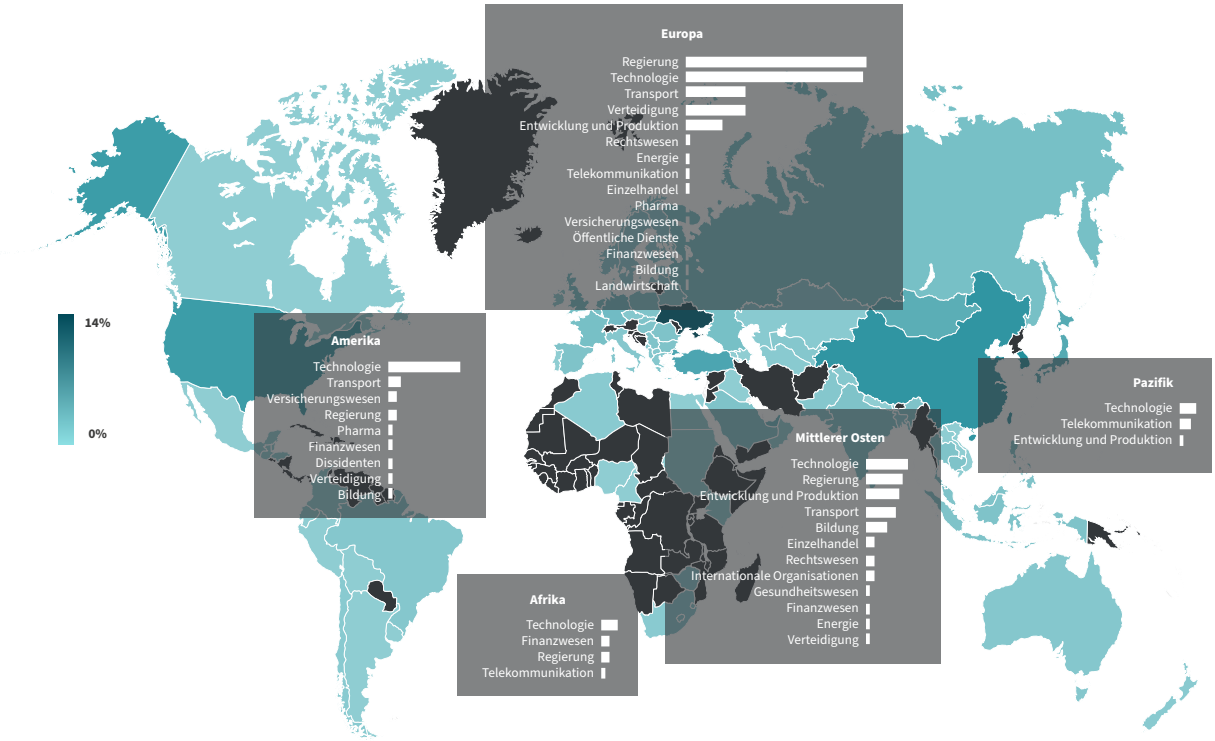
Cybersicherheit geht heute weit über den Schutz von Netzwerken und Geräten hinaus. Im Finanzsektor können Angriffe auf Zahlungssysteme oder sensible Daten in Nullkommanichts globale Auswirkungen haben. Im Gesundheitswesen und in den Life Sciences gefährden Sicherheitsverletzungen Patientinnen und Patienten direkt. In der Industrie und bei kritischen Infrastrukturen drohen Störungen des laufenden Betriebs oder sogar Sicherheitsrisiken. Branchenübergreifend nutzen Angriffe Komplexität, Geschwindigkeit und menschliche Fehler aus – und die Konsequenzen sind heute gravierender denn je.



Gemäss ENISA Threat Landscape Bericht 2025 ist der Finanzsektor in Europa das dritthäufigste Angriffsziel. 46 Prozent der Angriffe betreffen europäische Banken, gefolgt von öffentlichen Finanzorganisationen mit 13 Prozent.

Unsicherheit verstärkt diese Risiken zusätzlich. Geopolitische Spannungen können staatlich unterstützte Angriffe auslösen. Gleichzeitig werden Angriffsmethoden immer ausgefeilter. Das Ergebnis ist eine Bedrohungslage, die volatiler und schwerer einschätzbar ist als je zuvor. Das World Economic Forum berichtet, dass *72 Prozent der Führungskräfte weltweit geopolitische Ereignisse inzwischen in ihre Cybersicherheitsstrategien einbeziehen.* Gleichzeitig führen wirtschaftlicher Druck und Kostenziele dazu, dass digitale Projekte beschleunigt realisiert werden – teilweise zulasten sorgfältiger Sicherheitsmassnahmen. Abhängigkeiten in Lieferketten und die Nutzung von Cloud-Diensten schaffen weitere Angriffsflächen. Und während sich Technologien weiterentwickeln, passen sich auch Angreifer kontinuierlich an und nutzen neue Einstiegspunkte, zum Beispiel über KI, IoT oder Remote-Arbeitsumgebungen.

Die weltweit am häufigsten angegriffenen Branchen



Quelle: ESET - APT Report 2024-2025

Cybersicherheit als strategische Fähigkeit

Deshalb muss Cybersicherheit als strategische Fähigkeit verstanden werden, und nicht als rein reaktive Massnahme. Proaktive Sicherheit in der Softwareentwicklung, umfassende Tests von Anwendungen sowie die Einhaltung neuer regulatorischer Vorgaben wie dem Cyber Resilience Act sind heute keine Option mehr, sondern eine Voraussetzung für Resilienz und Vertrauen. Organisationen, die Sicherheit systematisch in ihre Prozesse integrieren, in defensive und offensive Skills investieren und eine vorausschauende Perspektive einnehmen, bleiben so auch in unsicheren Zeiten handlungsfähig.

Vernetzte Systeme, tatsächliche Auswirkungen

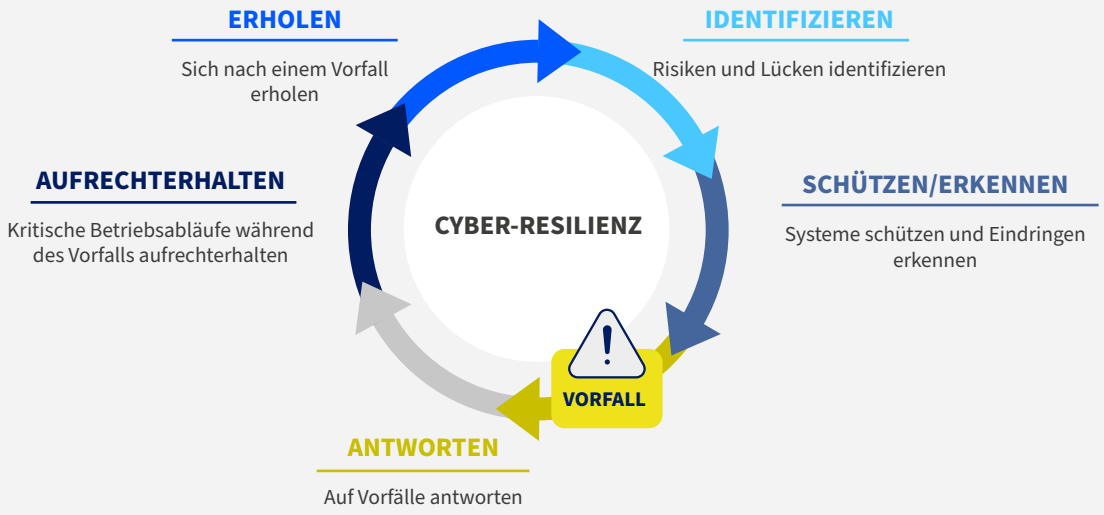
Heutzutage funktionieren Produkte nur selten isoliert. Vielmehr sind sie Teil komplexer Ökosysteme, die unseren Alltag direkt beeinflussen. Smart Homes benötigen sichere Schnittstellen, um Privatsphäre und Komfort zu schützen. Medizinische Geräte müssen zuverlässig kommunizieren, um die Patientensicherheit zu gewährleisten. Industrielle Systeme sind auf sichere Automatisierung angewiesen, um Ausfälle und Produktionsverluste zu vermeiden. Fahrzeuge tauschen kontinuierlich Daten aus, um Sicherheit in Echtzeit zu ermöglichen.

In all diesen Branchen ist Vertrauen eine Selbstverständlichkeit. Aber nur, bis es verletzt wird. Wenn Sicherheit versagt, sind die Auswirkungen sofort spürbar. Regulierungen wie der Cyber Resilience Act zielen darauf ab, Sicherheit über den gesamten Produktlebenszyklus hinweg sichtbar, messbar und wartbar zu machen. Der Fokus verschiebt sich von einzelnen Kontrollen zu systemischer Resilienz.

Wie Resilienz in der Praxis aussieht

Robuste Systeme entstehen nicht zufällig. Sie sind das Ergebnis bewusster Designentscheidungen und einer disziplinierten Umsetzung. Sicherheit muss von Anfang an berücksichtigt werden, durch Bedrohungsszenarien

5 Stufen der Cyber-Resilienz



Quelle: Weforum.org/stories/2022/07/how-do-you-safeguard-a-city-from-cyber-attacks/

und Modelle, klar definierte Sicherheitsanforderungen und die Einhaltung relevanter Standards. Entscheidungen, die während der Entwurfsphase getroffen werden, bestimmen oft, ob Sicherheit später ein Wegbereiter oder ein Hindernis ist.

Ebenso wichtig ist es, Sicherheit in die täglichen Entwicklungsabläufe zu integrieren. Durch standardmässig sichere Architekturen, Software-Stücklisten und CI-integrierte Schwachstellen-Scans können Teams Risiken kontinuierlich und nicht nur reaktiv angehen. Sicherheit wird zu einem Teil der Softwareentwicklung und nicht zu etwas, das am Ende hinzugefügt wird.

Resilienz reicht über das Release hinaus. Sichere Bereitstellung, Überwachbarkeit, Patch Management und Monitoring sind unerlässlich, um die operative Integrität langfristig aufrechtzuerhalten. Kontinuierliche Prüfungen durch Penetrationstests, simulierte Cyberangriffe (Red Teaming) und proaktive Bewertungen stellen sicher, dass Risiken sichtbar, beherrschbar und reduzierbar bleiben, während sich die Systeme weiterentwickeln.

Fazit

Diese Ausgabe von .experience befasst sich mit dem gesamten Spektrum der Herausforderungen und Antworten im Bereich Cybersicherheit. Sie erfahren, wie sichere Entwicklungspraktiken Schwachstellen vermeiden, wie regulatorische Rahmenbedingungen Verantwortlichkeiten gestalten und wie offensive Tests Einblicke in reale Risiken liefern. Dies wird anhand einer Geschichte mit drei Charakteren veranschaulicht – dem Guten (Entwickler), dem Bösen (ethischer Hacker) und dem Hässlichen (Compliance-Spezialisten).

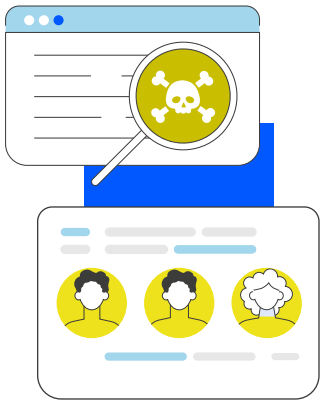
Über Albert Alsina

Albert Alsina ist Geschäftsführer von ERNI Spanien und verfügt über 10 Jahre Erfahrung bei ERNI in den Bereichen Projektleitung, Kundenmanagement und Talentförderung. Er leitet fast 300 Mitarbeitende und fördert Wachstum, Innovation und Projekte mit Impact. Albert engagiert sich leidenschaftlich für die Stärkung von Teams und bringt Arbeit, Familie, Sport, Musik und Kochen unter einen Hut.

«Das Gute, das Hässliche und das Böse»: Eine moderne Fabel über Cybersicherheit

Cybersicherheit ist in einer Welt voller Komplexität und neuer Bedrohungen eine gemeinsame Verantwortung. Für die Sicherheit von Systemen arbeiten Entwickler, ethische Hacker und Compliance-Spezialisten zusammen. In diesem Artikel erzählen wir die Geschichte von «dem Guten, dem Hässlichen und dem Bösen» in einer sicherheitsbewussten Organisation.

Von David Soto Dalmau, Cybersecurity Principal, ERNI Spanien



Ein klassischer Western ist zeitlos. Ein einsamer Cowboy reitet durch eine karge Landschaft, hinter jedem Felsen lauert Gefahr, Vertrauen ist so rar wie Wasser in der Wüste. Waffen werden gezogen, Vereinbarungen gebrochen, das Überleben hängt nicht nur davon ab, wer am schnellsten zieht, sondern auch davon, wer das Spiel versteht.

Tauschen Sie die Colts gegen Laptops und die staubigen Städte gegen Netzwerke und Systeme aus – und plötzlich scheint der Wilde Westen gar nicht mehr so fern.

In der Cybersicherheit bewegen wir uns, ähnlich wie in alten Westernfilmen, in einem unbekannten Grenzgebiet. Bedrohungen tauchen unangekündigt auf. Verbündete können sich abwenden. Und beim Sieg geht es nicht um rohe Gewalt – es geht darum, den Gegner zu überlisten, sein Revier zu schützen und zu wissen, wann man schiessen und wann man programmieren muss.

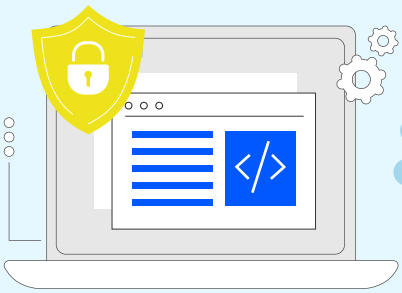
Bei ERNI sind wir uns dieser Dynamik bewusst. Jeder Kundenauftrag ist wie eine neue Stadt mit eigenen Regeln, einem Sheriff und eigenen Gefahren, die überall lauern. Deshalb gehen wir jedes Projekt mit einem Expertentrio an: «dem Guten, dem Hässlichen und dem Bösen». Jeder hat seinen Zweck, jeder hat seine Rolle, und keiner ist ohne die anderen wirklich effektiv.

Das ist nicht nur eine Metapher, es ist eine Methode. Und genau das ist es, was unseren Ansatz beim Aufbau, der Regulierung und dem Testen sicherer Systeme in der digitalen Welt leitet, die sich oft so gesetzlos anfühlt wie der Wilde Westen.

Und an dieser Grenze beginnt unsere Geschichte

In einem weit entfernten digitalen Wilden Westen, wo Firewalls die neuen Viehzäune sind und Kopfgeldjäger «Pentester» (Penetrationstester) genannt werden, reiten drei Gestalten in die Cybersicherheits-Grenzzone: «das Gute, das Hässliche und das Böse». Dies ist keine Geschichte über Schiessereien um 12 Uhr mittags, sondern über simulierte Angriffe, langwierige Vorschriften und unbesungene Helden, die nach Prinzipien programmieren. Ein Paradoxon: Um uns vor dem Chaos zu schützen, brauchen wir ein wenig Chaos, eine Prise Gesetz und einen Wächter, der weiss, wann er Code schreiben muss.

Das Gute: **Sichere Entwicklung**



Die Guten tragen einen digitalen Laborkittel, trinken viel Kaffee und schreiben sauberen Code. Sie sind die, die von Anfang an Sicherheit gestalten, indem sie die Prinzipien von «Secure by Design» anwenden und jede Komponente, jede Abhängigkeit und jeden Endpunkt überprüfen.

Ihre Ethik basiert auf Professionalität, nicht auf Angst vor Auditoren oder Angreifern, sondern auf Respekt gegenüber den Nutzerinnen und Nutzern.

Die Guten dokumentieren, validieren Eingaben, verschlüsseln die Kommunikation und sehen voraus, was schiefgehen könnte, bevor es passiert. Sie stützen sich auf Modelle wie STRIDE, verwenden SAST- und DAST-Tools und folgen Frameworks wie OWASP ASVS.

Aber sie haben auch die Seele eines Geschichtenerzählers: sie erzählen eine Geschichte von Vorsorge, intelligentem Design und Verantwortung.

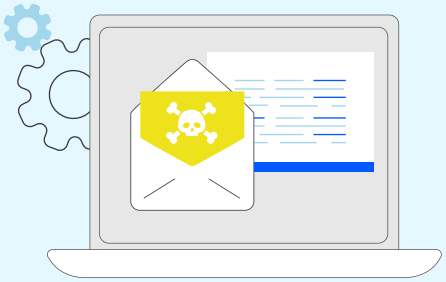
Das Hässliche: **Vorschriften, die niemand will**

Die Hässlichen tragen graue Anzüge und Klemmbretter. Sie sprechen über DSGVO, ISO 27001, NIS2 und andere Abkürzungen, die Tech-Teams ins Schwitzen bringen. Sie sind Auditoren, Compliance-Beauftragte und Risikomanager. Niemand lädt sie zu Kreativmeetings ein, aber alle melden sich, wenn etwas kaputt geht.

Ihre Hässlichkeit liegt nicht in ihrer Funktion, sondern in ihrer Wahrnehmung: Sie werden als Last und nicht als Schutz angesehen.

Das Hässliche verkörpert das griechische Wort Logos, das Rationalität, Strukturen, Kontrollen und Prozesse auferlegt. Es verlangt Verschlüsselungsnachweise, Zugriffskontrollen und Schwachstellenmanagement. Ja, manchmal fühlt es sich wie Bürokratie an, aber ohne es gäbe es keine Grenzen, keine Rechenschaftspflicht, keine Gerechtigkeit, wenn Systeme versagen. Das Hässliche verwandelt «wir sollten» in «wir müssen» – unpopulär, aber unverzichtbar.

Das Böse: **Die ethischen Hacker**



Das Böse schlüpft mit einem schiefen Grinsen durch die Hintertür. Es trägt Kapuzenpullis, arbeitet an dunklen Terminals und stellt unbequeme Fragen. Es sind die Pentester im Red Team, die offensiven Cybersicherheitsberater. Ihre Aufgabe: ihren eigenen Kunden anzugreifen.

Von aussen wirken sie wie Bösewichte, aber sie handeln ethisch: Fehler finden, bevor echte Bösewichte die Schwachstellen entdecken.

Das Böse vermittelt Pathos: die Dringlichkeit, die unmittelbare Gefahr, das Adrenalin, das uns daran erinnert, dass kein System unverwundbar ist.

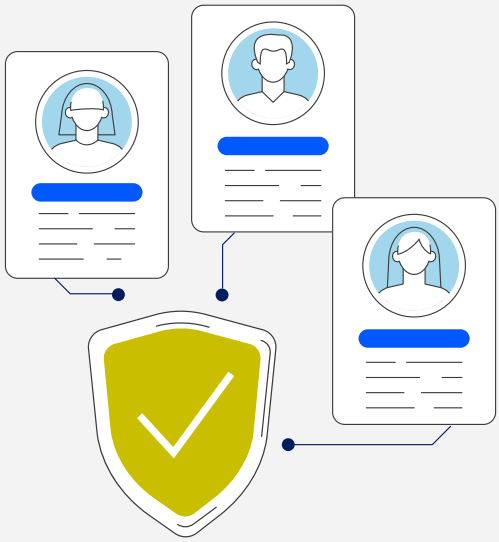
Es nutzt Metasploit, Burp Suite, benutzerdefinierte Skripte und jede Menge Kreativität. Es macht Dinge kaputt, damit andere sie reparieren können. Auch wenn es manchmal das Gute nervt oder das Hässliche irritiert, ist es für den Abschluss des Sicherheitszyklus unverzichtbar.

Ein zirkuläres Paradoxon

Das Gute baut sichere Systeme, kann aber nicht alles vorhersehen. Das Böse testet sie und sucht nach dem einen Prozent menschlicher oder technischer Fehler. Das Hässliche beobachtet, dokumentiert, setzt durch und sorgt dafür, dass die Lektionen nicht vergessen werden.

Aber es ist auch wahr, dass ohne das Gute das Böse nur Ruinen vorfinden würde; ohne das Böse würde das Gute in falscher Zuversicht leben; und ohne das Hässliche würde alles, was man lernt, im Chaos der Sprints verloren gehen.

Es ist paradox, dass diese Drei einander brauchen, einander herausfordern und ergänzen. Ohne Design, Validierung und Compliance gibt es keine Sicherheit. Und ohne die Akzeptanz, dass das Böse vielleicht richtig ist, und das Hässliche – auch wenn es nervt – das schützt, was das Gute aufbaut, gibt es keinen Fortschritt.



Der ERNI-Ansatz: Wenn die drei zusammen reiten

Bei ERNI erzählen wir diese Geschichte nicht nur, wir leben sie auch. Unser Ansatz zur Cybersicherheit integriert diese drei Archetypen in unser Servicemodell und passt sie an die realen Bedürfnisse unserer Kunden an.

Wenn unsere Kunden robuste, zukunftssichere digitale Produkte benötigen, bringen wir das Beste ins Spiel: unsere sicheren Softwareentwicklungsteams, die Best Practices anwenden, von Code Reviews bis hin zu Bedrohungsmodellierung, und so sicherstellen, dass Sicherheit vom ersten Tag an integriert ist.

Wenn Compliance zu einem kritischen Faktor wird, sei es im Gesundheitswesen, im Finanzwesen oder in der öffentlichen Infrastruktur, kommt das Hässliche ins Spiel. Unsere Expertinnen und Experten für Regulierung und Governance führen Unternehmen durch das Labyrinth der gesetzlichen und industriellen Anforderungen. Sie haken nicht einfach nur Checklisten ab, sondern entwickeln Systeme, die überprüfbar, zuverlässig und widerstandsfähig sind.

Und wenn Kunden ihre Annahmen hinterfragen und ihre Abwehrmassnahmen verbessern möchten, kommt das Böse zum Einsatz. Unsere Offensive Security Teams führen ethisches Hacking und Red Teaming durch und simulieren reale Bedrohungen, um Grenzen zu testen und Schwachstellen aufzudecken.

Jede Rolle ist für sich genommen wertvoll, aber wir bei ERNI wissen, dass ihre grösste Stärke in ihrer Synergie liegt. Wir passen dieses Trio an die Reife, die Bedürfnisse und die Branche jedes Kunden an – manchmal beginnen wir mit dem Hässlichen, um grundlegendes Vertrauen aufzubauen, manchmal setzen wir das Böse ein, um Angriffsflächen zu identifizieren, oder lassen das Gute ein neues Produkt mit integrierter Sicherheit entwickeln.

Wir glauben, dass Sicherheit nicht nur eine Funktion ist, sondern eine Praxis. Indem wir alle drei Perspektiven berücksichtigen, helfen wir Unternehmen nicht nur, sich zu verteidigen, sondern auch, mit Zuversicht in einer digitalen Welt zu wachsen, die sich schneller verändert als ein Revolverheld ziehen kann.

Epilog: Ein vermiedenes Duell

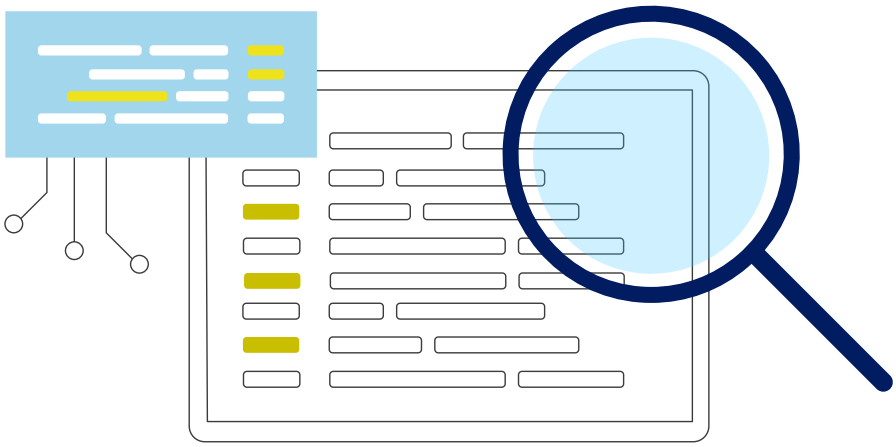
In dieser Geschichte gibt es kein finales Duell. Das Gute erschiesst das Böse nicht, und das Hässliche legt niemandem Handschellen an. Stattdessen arbeiten sie zusammen: Das Gute programmiert mit Weitsicht, das Böse testet mit List, und das Hässliche schreibt die Spielregeln.

Die Moral ist einfach: Effektive Cybersicherheit wird nicht dadurch erreicht, dass man das Böse beseitigt oder das Hässliche ignoriert. Sie wird erreicht, wenn alle drei verstehen, dass sie zusammenarbeiten müssen, damit die digitale Welt florieren kann.

Fragen Sie sich «Wo sind meine drei Gesetzlosen?», wenn Sie das nächste Mal über Sicherheit nachdenken. Denn wenn einer fehlt, könnte jemand anderes schneller ziehen.

Nächste Folge: An die Front

Dies war nur die Eröffnungsszene. In den nächsten Artikeln werden wir tiefer in das Gebiet jeder dieser drei Figuren eintauchen. Wir werden ihre Werkzeuge, ihre Denkweise und ihren Ehrenkodex erkunden. Anhand von Fällen aus der realen Welt werden wir sehen, wie das Gute aufbaut, wie das Hässliche regiert und wie das Böse zerstört. Machen Sie sich bereit. Die Geschichte fängt gerade erst an.



Über David Soto Dalmau

David Soto Dalmau ist Leiter des Bereichs Cybersicherheit bei ERNI in Barcelona. Als lebenslanger Enthusiast für ethisches Hacking und Capture the Flag (CTF) kombiniert er Fachwissen in Kryptografie, Penetrationstests und Risikomanagement mit der Vermittlung und Förderung einer Kultur des kontinuierlichen Lernens.

«Ich bin kein Held – ich entwickele sichere Software»

In einer Welt, die von rasanten digitalen Entwicklungen und ständigen Cyber-Bedrohungen geprägt ist, verfolgt das Gute einen anderen Ansatz. Die Guten sind weder die schnellsten Programmierer noch die lautesten Stimmen, aber ihre Arbeit sorgt oft für die Sicherheit von Systemen. In diesem Exklusivinterview untersuchen wir, was es heute wirklich bedeutet, sichere Software zu entwickeln.

Ein Interview mit dem Guten (Samuel Hernández, Full-Stack-Experte bei ERNI Spanien) an der digitalen Front

.experience: Wie definierst du deine Rolle in einem Entwicklungsteam?

Das Gute: Ich sehe mich als den, der dafür sorgt, dass das Fundament solide ist, bevor das Haus gebaut wird. Meine Aufgabe ist es, vorauszudenken. Nicht nur, um Funktionalität zu liefern, sondern um zu antizipieren, was schiefgehen könnte, und Schutzmassnahmen zu ergreifen, bevor der Code ausgeführt wird. Ich arbeite daran, sicherzustellen, dass das, was wir liefern, nicht nur leistungsfähig oder skalierbar ist, sondern auch von Grund auf sicher. Es geht weniger darum, Angriffe reaktiv zu verhindern, als vielmehr darum, Systeme zu entwickeln, die von Anfang an widerstandsfähig sind.

Wann kommt Sicherheit im Prozess ins Spiel?

Vor dem ersten Commit. Sicherheit beginnt mit der Architektur. Bevor wir mit dem Programmieren anfangen, möchte ich wissen, mit welchen Daten wir arbeiten, wo sie gespeichert sind, wer darauf Zugriff hat und was schiefgehen könnte. Ich verwende Frameworks zur Bedrohungsmodellierung wie STRIDE, um potenzielle Schwachstellen zu visualisieren und Massnahmen direkt

in das Design einzubauen, um sie zu minimieren. Wenn Sicherheit erst nachträglich berücksichtigt wird, entsteht eine technische Schuldenlast. Meine Aufgabe ist es, sie von Anfang an einzubauen.

Kannst du uns deine täglichen Helfer vorstellen?

Meine Tools verändern sich je nach Projektphase, aber einige Grundelemente bleiben bestehen. In der frühen Entwicklungsphase definiere ich Codierungsstandards, die die häufigsten Fehler wie keine fest codierten Anmeldedaten, keine ungeprüften Eingaben oder keine unsicheren Abhängigkeiten vermeiden. Parallel dazu implementiere ich statische Analyse-Tools (SAST), die den Code bei jedem Push scannen. Während der Integration füge ich dynamische Analysen (DAST) hinzu, um Live-Anwendungen auf Verhaltensprobleme zu testen. Ausserdem verlasse ich mich auf Infrastructure-as-Code-Validierungen und Containerscans, um sicherzustellen, dass die Bereitstellungsumgebungen genauso vertrauenswürdig sind wie der Code selbst.

Ich verwende Abhängigkeitsscanner, die mit öffentlichen Schwachstellendatenbanken verknüpft sind, und führe für jeden Build eine detaillierte Software-Stückliste (SBOM). Jedes von uns verwendete Paket wird erfasst, versioniert und überwacht. Wenn in einer Upstream-Bibliothek eine Schwachstelle entdeckt wird, wissen wir bereits genau, wo sie sich in unserem System befindet.

Wie stehst du zum Thema Geheimnisse und Zugangsdatenverwaltung?

Geheime Informationen sollten niemals sichtbar sein. Keine Passwörter im Klartext, keine API-Schlüssel, die in Speichern abgelegt werden. Ich integriere Tools zur Verwaltung geheimer Informationen wie Vault oder Cloud-native Lösungen, um sensible Daten verschlüsselt und zugriffskontrolliert zu halten. Dabei wende ich konsequent das Prinzip der geringsten Privilegien an. Kein Benutzer und kein Prozess sollte mehr Zugriff haben als unbedingt notwendig. Ausserdem automatisiere ich die Umstellung geheimer Informationen und überwache Zugriffsprotokolle. Geheime Informationen werden wie Waffen behandelt: unter Verschluss gehalten, sorgfältig nachverfolgt und nur bei Bedarf verwendet.

Was macht einen sicheren Entwickler aus, abgesehen von Tools und Code?

Disziplin. Bei der sicheren Entwicklung geht es nicht darum, jeden Schwachpunkt zu kennen, sondern methodisch vorzugehen. Es geht darum, bei jedem Schritt bewusste Entscheidungen zu treffen: Eingaben validieren, Typsicherheit durchsetzen, verantwortungsbewusst protokollieren, über Fehlermodi nachdenken. Ich investiere auch Zeit in die Dokumentation, nicht nur für mein Team, sondern für alle, die den Code morgen übernehmen. Sicherheit lebt von Klarheit, und durch Dokumentation geben wir Absichten und Warnungen weiter.

Aber darüber hinaus geht es um Kultur. Ich setze mich für sichere Praktiken bei Code-Reviews ein. Dazu veranstalte ich Retrospektiven, bei denen es nicht um Schuldzuweisungen geht, sondern darum, zu lernen. Ich schule meine Teamkolleginnen und -kollegen darin, Warnsignale zu erkennen. Mein Ziel ist es nicht, der Einzige zu sein, der sich Gedanken über Sicherheit macht – ich möchte sicherstellen, dass sich alle Gedanken darüber machen.

Wie gehst du mit Legacy-Systemen oder unsicheren Vererbungen um?

Mit Geduld und einer klaren Strategie. Ich beginne damit, das System zu untersuchen und Bereiche mit erhöhtem Risiko zu identifizieren. Anschliessend führe ich eine Einstufung durch: Was muss sofort behoben werden, was kann gemildert werden und was sollte abgeschafft werden? Ich konzentriere mich auf Isolierung, Eingabevalidierung und das Patchen, was möglich ist, während ich mich bei Bedarf für eine langfristige Neugestaltung einsetze. Das ist nie ideal, aber Legacy-Systeme sind nun einmal Realität. Der Schlüssel liegt darin, ihre Angriffsfläche schrittweise zu reduzieren, ohne die Produkt-Roadmap zu beeinträchtigen.

Wie sieht Erfolg für jemanden in deiner Position aus?

Ironischerweise bedeutet Erfolg oft Stille. Keine Sicherheitsverletzungen. Keine dringenden Hotfixes. Keine Schlagzeilen. Es bedeutet, dass Systeme einfach laufen – und weiter funktionieren, ohne dass die Benutzer jemals bemerken, wie viele Dinge hätten schiefgehen können, aber nicht schiefgegangen sind. Es bedeutet auch, dass wir wissen, dass wir über Protokolle, Warnmeldungen und Rollback-Mechanismen verfügen, falls doch einmal etwas schiefgeht. Wenn alles glatt läuft, wird es als selbstverständlich gesehen.

Gibt es Missverständnisse über sichere Entwicklung, denen du oft begegnest?

Ja, jede Menge. Das grösste ist, dass sichere Entwicklung langsam ist. Das mag so erscheinen, insbesondere in Teams, die Geschwindigkeit über Struktur stellen, aber langfristig gesehen ist sie sogar schneller. Man vermeidet Brandbekämpfung. Man reduziert Nacharbeit. Man baut Vertrauen bei Kunden und Aufsichtsbehörden auf. Ein weiterer Mythos ist, dass Sicherheit die Aufgabe anderer ist, in der Regel eines externen Teams oder eines Prüfers. Das lehne ich entschieden ab. Sicherheit ist die Aufgabe aller, aber Entwicklerinnen und Entwickler stehen an vorderster Front. Wir haben die Möglichkeit, vorbeugend zu handeln und nicht nur zu reagieren.

Wie hältst du die Balance zwischen Sicherheit und dem Druck, Produkte fertig zu stellen und Termine einzuhalten?

Das ist einer der schwierigsten Aspekte meiner Arbeit. Der Druck, schnell Ergebnisse zu liefern, ist gross, und Sicherheit wird von Aussenstehenden oft als Hindernis betrachtet. Ich versuche daher, Sicherheit in bestehende Arbeitsabläufe zu integrieren, damit sie nicht zum Stolperstein wird. Automatisierte Tests, Pre-Commit-Hooks und einfache Überprüfungen sind dabei sehr hilfreich. Aber ich arbeite auch daran, Glaubwürdigkeit aufzubauen. Wenn Teams sehen, dass ich nicht nur auf Probleme hinweise, sondern dazu beitrage, künftiges Chaos zu verhindern, beginnen sie, diesen Beitrag zu schätzen. Das Gleichgewicht entsteht durch Partnerschaft, nicht durch Zwang.

Bist du jemals gescheitert? Und was hast du daraus gelernt?

Auf jeden Fall. Ich habe Dinge übersehen. Das passiert uns allen. Einmal hat ein Drittanbieterpaket, dem ich vertraut habe, eine kritische Sicherheitslücke in einem Patch-Release verursacht. Ich hatte ein SBOM, aber ich habe die Versionssperren nicht streng genug durchgesetzt. Wir haben das Problem schnell entdeckt, aber es war ein Weckruf. Seitdem gehe ich mit Code von Drittanbietern noch kritischer um. Aus Fehlern lernt man, zurückhaltend zu sein – und man lernt, mehr auf seine Systeme, seine Warnmeldungen und seine Intuition zu hören.

> Der Druck, schnell Ergebnisse zu liefern, ist gross, und Sicherheit wird von Aussenstehenden oft als Hindernis betrachtet. Ich versuche daher, Sicherheit in bestehende Arbeitsabläufe zu integrieren, damit sie nicht zum Stolperstein wird.

Was motiviert dich, diese Arbeit weiterzumachen?

Ich glaube, dass Technologie eine immense Kraft hat, aber damit gehen auch enorme Risiken einher. Allzu oft bauen wir zuerst und denken erst später darüber nach. Ich möchte nicht in einer Welt leben, in der Sicherheit erst dann gilt, wenn jemand zu Schaden gekommen ist. Vielmehr möchte ich Dinge entwickeln, die Menschen befähigen, ohne sie zu gefährden. Das ist es, was mich antreibt. Das Wissen, dass ruhige, durchdachte Arbeit heute die Zukunft anderer Menschen schützen kann.

Was unterscheidet einen Cybersicherheitsexperten von anderen Entwicklern?

Cybersecurity Champions sind nicht nur Leute, die wissen, wie man sicheren Code schreibt – sie bringen diese Denkweise ins Team ein und setzen sich konsequent dafür ein. Was sie auszeichnet, ist nicht ihre technische Brillanz, sondern ihre Präsenz. Sie sind die, die bei der Sprint-Planung unbequeme Fragen stellen, die ihre Hand heben, wenn eine Abkürzung zu einem Risiko werden könnte. Sie beheben nicht nur Schwachstellen, sondern tragen dazu bei, deren Wiederauftreten zu verhindern. Champions schlagen Brücken zwischen Entwicklern und Entwicklerinnen und Sicherheitsexperten und -expertinnen, zwischen dem Unternehmen und der Technik. Sie schaffen eine Kultur, in der Sicherheit Teil der Definition of Done ist.

Cybersecurity Champions sind nicht nur Leute, die wissen, wie man sicheren Code schreibt – sie bringen diese Denkweise ins Team ein und setzen sich konsequent dafür ein.

Abschliessende Gedanken?

Ich bin kein Held. Also jage ich keine Gefahren und suche auch nicht nach Ruhm. Ich baue auf Beständigkeit. Meine Aufgabe ist es, dafür zu sorgen, dass man dem, was wir entwickeln, vertrauen kann. Denn am Ende ist Vertrauen die wertvollste Währung in der Tech-Branche. Und das verdient man sich Schritt für Schritt.

Über Samuel Hernández

Samuel Hernández, unser Full-Stack-Experte bei ERNI Spanien, entwickelt Lösungen, die medizinische Geräte mit Laborsystemen verbinden, unter Verwendung von .NET, Angular, Cloud-Technologien und sicheren, konformen Verfahren. Mit seiner Leidenschaft für Innovation und zuverlässige Software sorgt er für hochwertige, benutzerorientierte Lösungen in komplexen, regulierten Umgebungen.

Ein 360°-Ansatz: Security Best Practices für professionelle Entwicklungsteams

Sicherheit ist mehr als eine Checkliste. Dieser Fall zeigt, wie wir einen 360°-Ansatz für professionelle Entwicklungsteams eingeführt haben, der Prinzipien, Best Practices und die Durchsetzung von CI-/CD-Vorgaben kombiniert. Die Teams gewannen an Klarheit, Selbstvertrauen und Abstimmung, sodass Sicherheit zu einem selbstverständlichen Teil der Softwarequalität wurde.

Von David Soto Dalmau, Cybersecurity Principal, ERNI Spanien

Die Herausforderung: Sicherheitswissen ohne einheitlichen Rahmen

In vielen Unternehmen entwickeln sich Initiativen zur Softwaresicherheit organisch. Die Teams erhalten Anleitungen zu Datenschutz, Codierungsstandards, Schwachstellenmanagement und Tools oft als isolierte Themen, die voneinander losgelöst sind.

Das Ergebnis ist bekannt: Entwicklerinnen und Entwickler wissen, welche Tools sie verwenden und welche Regeln sie befolgen müssen, haben jedoch Schwierigkeiten zu verstehen, wie alle Sicherheitsaspekte über den gesamten Software-Lebenszyklus hinweg zusammenhängen.

Das zentrale Anliegen unserer Schulungsinitiative bestand daher nicht darin, mehr Kontrollen einzuführen, sondern ein gemeinsames, durchgängiges Sicherheitsmodell zu etablieren, das die Entwicklungsteams einheitlich anwenden können – von Designentscheidungen bis hin zum Laufzeitverhalten.

Die 360°-Sicht: Sicherheit als kontinuierliches System

Von Anfang an war das Training auf eine einzige Idee ausgerichtet: Sichere Software lässt sich nicht durch eine einzelne Massnahme oder ein einzelnes Tool erreichen, sondern durch die Abstimmung von Grundsätzen, Verhaltensweisen und Kontrollen über den gesamten Entwicklungslebenszyklus hinweg.

Um dies greifbar zu machen, haben wir das Programm als Reise mit drei Dimensionen, die sich ergänzen, strukturiert:

- Grundlegende Sicherheitsprinzipien
- Bewährte Verfahren für sichere Entwicklung
- Operative Sicherheitskontrollen, integriert in CI/CD

Jede Ebene verstärkte die nächste und schuf so ein kohärentes und wiederholbares Sicherheitbewusstsein.

Grundlagen: die CIA-Triade als Sicherheitsgrundlage

Die Reise begann mit den Grundprinzipien. Anstatt direkt mit Tools zu beginnen, wurde im Rahmen der Schulung zunächst eine gemeinsame Grundlage anhand der CIA-Triade – Vertraulichkeit, Integrität und Verfügbarkeit – geschaffen.

Dies wurde nicht theoretisch betrachtet, sondern aus einem praxisorientierten Blickwinkel, durch den alle späteren Entscheidungen bewertet werden sollten:

- Welche Daten müssen vertraulich bleiben?
- Welche Vorgänge erfordern Integritätsgarantien?
- Von welchen Verfügbarkeitsannahmen hängt das System ab?

Durch die Verankerung von Sicherheitsdiskussionen in CIA erhielten die Teams eine neutrale, technologieunabhängige Methode, um Risiken und Auswirkungen unabhängig von Implementierungsdetails zu bewerten.

Diese Grundlage erwies sich später bei der Erörterung von Kompromissen, Prioritäten und Fehlerszenarien als unverzichtbar.

Best Practices für sichere Entwicklung: von den Grundsätzen zum Verhalten

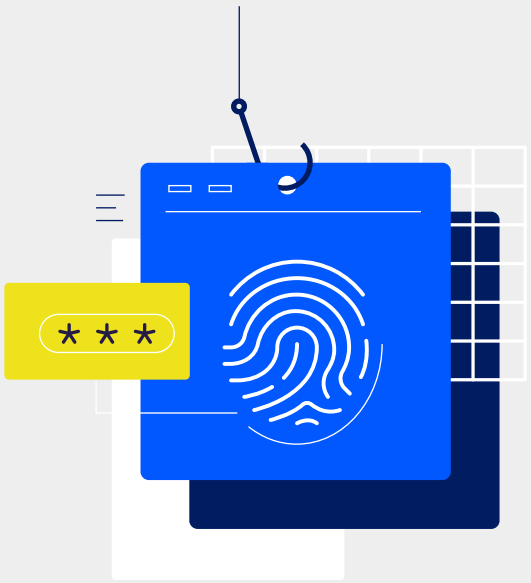
Aufbauend auf der CIA-Triade konzentrierte sich der zweite Teil der Schulung auf sichere Entwicklungspraktiken, wobei Sicherheit als Qualitätsmerkmal von Software behandelt wurde, gleichwertig mit Leistung oder Zuverlässigkeit. Zu den wichtigsten Themen gehörten:

- Eingabevalidierung als explizite Vertrauensgrenze
- Sichere Handhabung von Geheimnissen und sensiblen Daten

- Sitzungsmanagement und Autorisierungsinvarianten
- Zero-Trust-Prinzipien auf Code-Ebene

Der Schwerpunkt lag bewusst auf dem Verhalten der Entwicklerinnen und Entwickler und nicht auf Checklisten. Sicherheit wurde als eine Reihe von Invarianten definiert, die unabhängig von Refactoring, Funktionserweiterungen oder architektonischen Weiterentwicklungen gelten müssen.

Dieser Ansatz half den Teams zu erkennen, dass viele Vorfälle in der Praxis nicht durch exotische Angriffe verursacht werden, sondern durch Regressionen. Das sind Kontrollen, die einst funktionierten, aber durch spätere Änderungen unbeabsichtigt ausser Kraft gesetzt wurden.



Von Best Practices zum Nachweis: testen und verifizieren

Nachdem sichere Codierungspraktiken etabliert waren, wandte sich die Schulung dem oft missverstandenen Bereich «Sicherheitstests im Vergleich zu Schwachstellenscans» zu. Wir haben eine klare Unterscheidung eingeführt:

- **Sicherheitstests** beweisen, dass Kontrollen unter Angriffsbedingungen funktionieren.
- **Schwachstellenscans** erkennen bekannte Risikoindikatoren in grossem Massstab.

Diese Unterscheidung beseitigte eine häufige Quelle falscher Zuversicht und schuf realistische Erwartungen für jede Werkzeugkategorie.

Sicherheitstests wurden als eine Möglichkeit zur Validierung des Verhaltens (negative Pfade, Missbrauchsfälle und Ausfallmodi) vorgestellt, während das Scannen als eine wichtige, aber ergänzende Signalquelle positioniert wurde.

Tool-Integration: Anpassung der Sicherheitskontrollen am Stack

Erst nachdem die Grundsätze und Praktiken klar waren, haben wir im Rahmen der Schulung Sicherheitswerkzeuge vorgestellt, die ausdrücklich auf den verwendeten Technologie-Stack abgestimmt waren.

Anstatt eine feste Werkzeugkette zu fördern, lag der Schwerpunkt auf diesen Fragen:

- **Warum** es ein Tool gibt
- **Wo** es im Lebenszyklus eingesetzt wird
- **Wann** es Lieferentscheidungen beeinflussen sollte

Statische Analyse, Abhängigkeits-Scans, SBOM-Generierung, Laufzeittests und Konfigurations-Scans wurden konkreten Pipeline-Phasen zugeordnet, wodurch die Konsistenz der Absicht auch über heterogene Technologien und Sprachen hinweg betont wurde.

Ein besonderer Schwerpunkt lag auf nicht verhandelbaren Risiken, wie beispielsweise durchgesickerten Geheimnissen oder kritischen Fehlkonfigurationen, die alle anderen Sicherheitsgarantien ungültig machen und immer sofortige Massnahmen erfordern.

Sicherheit durch die Pipeline gewährleistet

Der letzte Teil der Schulung fasste alles zu einem einzigen, funktionsfähigen Modell zusammen: kontinuierliche Sicherheit durch die gesamte Lieferkette hindurch.

Von Pull-Anfragen bis hin zu Umgebungen vor der Veröffentlichung war jede Phase mit diesen Aspekten verbunden:

- Eine bestimmte Art von Sicherheitssignal
- Eine klare Entscheidung (blockieren, verfolgen oder fortfahren)
- Explizites Ownership

Diese auf Pipelines ausgerichtete Sichtweise verwandelt Sicherheit von einem abstrakten Anliegen in ein wiederholbares Ausführungsmodell, das Teams visualisieren, diskutieren und weiterentwickeln können.

Ergebnis: Abstimmung, Klarheit und Vertrauen

Der ganzheitliche Ansatz der Schulung, der Prinzipien, Praktiken und Umsetzung umfasste, erwies sich als ihre grösste Stärke.

Das Feedback der Entwicklungsteams, kurz zusammengefasst:

- Ein klareres Verständnis dafür, warum Sicherheitskontrollen existieren
- Mehr Vertrauen in deren Anwendung
- Bessere Abstimmung zwischen Sicherheitserwartungen und technischer Realität

Vor allem wurde Sicherheit nicht mehr als externe Einschränkung wahrgenommen, sondern als integraler Bestandteil der professionellen Softwareentwicklung.

Fazit

Beim Übertragen von Best Practices im Bereich Sicherheit auf professionelle Entwicklungsteams geht es nicht darum, Regeln, Tools oder Compliance-Anforderungen zu transferieren. Es geht darum, ein kohärentes Sicherheitsmodell zu übertragen, das den gesamten Lebenszyklus umfasst.

Wenn Unternehmen sichere Entwicklung aus einer 360°-Perspektive angehen, basierend auf Prinzipien, gestützt durch Best Practices und durchgesetzt durch Automatisierung, ist Sicherheit nicht mehr nur eine Nebensache, sondern wird Teil der Entwicklung hochwertiger Software.

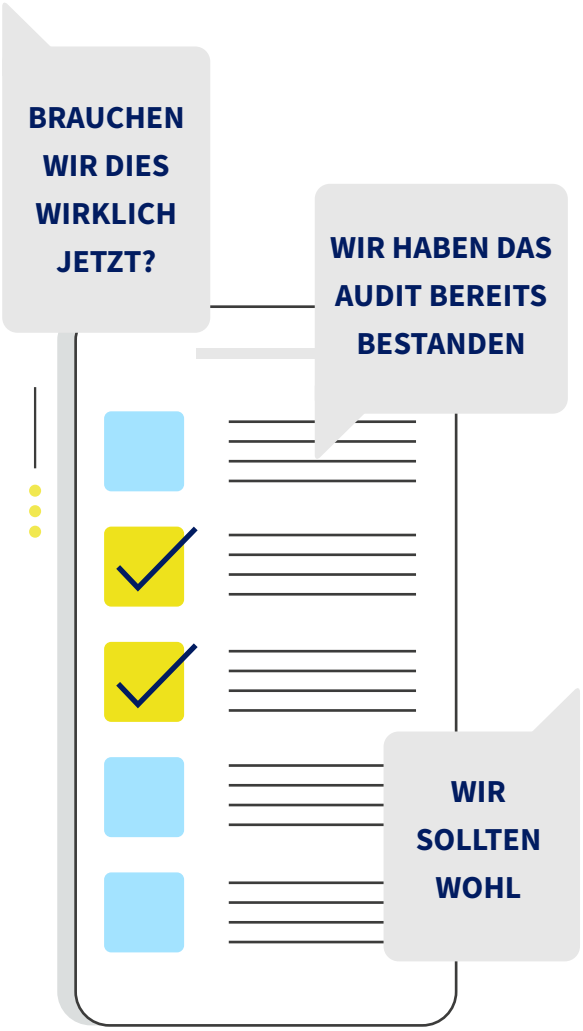
Über David Soto Dalmau

David Soto Dalmau ist Leiter des Bereichs Cybersicherheit bei ERNI in Barcelona. Als lebenslanger Enthusiast für ethisches Hacking und Capture the Flag (CTF) kombiniert er Fachwissen in Kryptografie, Penetrationstests und Risikomanagement mit der Vermittlung und Förderung einer Kultur des kontinuierlichen Lernens.

Die Sicht des Hässlichen: Warum Compliance nicht das ist, was Sie denken

Compliance spielt in der Cybersicherheit oft die Rolle des Buhmanns: Richtlinien, Audits und unangenehme Fragen, die niemandem gefallen. Aber hinter den Checklisten steckt Erfahrung, die auf die harte Tour gesammelt wurde. Dieser Artikel gibt dem Hässlichen das Wort und zeigt, warum es bei Compliance nicht um Kontrolle geht, sondern um den Schutz von Menschen, Produkten und um Vertrauen.

Von José Francisco Agulló, Quality Manager, ERNI Spanien



Ja, ich bin das Hässliche – und ich möchte, dass Sie verstehen, warum

Sie kennen diesen Typ Mensch. Die Person mit der Checkliste, die von ISO 27001, NIS2, DSGVO und CRA spricht. Der Compliance-Beauftragte, der von den Technikteams gemieden wird, die Risikomanagerin, die unangenehme Fragen stellt. Ich bin nicht bei den lustigen Brainstorming-Sitzungen dabei, aber ich bin in Ihren Gedanken, wenn etwas schief geht.

Ich verstehe, wie ich wirke: wie ein notwendiges Ärgernis, nicht wie ein cooler Teamkollege. Vielleicht erinnern Sie sich an all die Audit-Kontrollen, die ich immer wieder erwähne. Sie resultieren aus den Erfahrungen, was ohne sie passiert.

Die Forderung nach einem Verschlüsselungsnachweis sorgt für Datensicherheit. Zugriffsüberprüfungen verhindern, dass kleine Fehler zu grossen Problemen werden. Ich möchte einfach nur dazu beitragen, dass aus «wir sollten wahrscheinlich» etwas Konkretes wird. Das mag schwierig erscheinen, aber es dient dazu, alle zu unterstützen.

Die Blicke verstehe ich gut

Ich höre diesen leisen Seufzer, wenn ich eine neue Richtlinie vorstelle: «Brauchen wir das jetzt wirklich?».

- Entwicklerinnen und Entwickler fragen sich, ob die Eingabevalidierung nicht bis nach dem Start warten kann.
- Das Management ist der Meinung, dass MFA (Multi-Faktor-Authentifizierung) den Arbeitsalltag verlangsamt.
- Die Geschäftsleitung glaubt, dass wir durch das Zertifikat abgesichert sind.

Ich erlebe das auch. Wochenlang werden Risikobewertungen und Kontrollprüfungen durchgeführt, in der Hoffnung, dass alles klappt, nur um später Abkürzungen zu sehen, weil «wir das Audit bereits bestanden haben». Ich verstehe die Frustration. Aber bei dieser Arbeit geht es darum, das zu schützen, was uns allen am Herzen liegt.

Was ich aus den schwierigen Momenten gelernt habe

Ich erwähne das nicht, um Ihnen das Leben schwer zu machen. Ich habe die Kehrseite gesehen:

- Die versäumte Eingabeprüfung, die fehlerhafte Daten zulässt, die dem Kunden schaden.
- Der verspätete Patch, der zu stundenlangen Wiederherstellungsarbeiten führt.
- Der Anbieter, dem ohne Sicherheitsvorkehrungen vertraut wurde, und der alle mit in den Abgrund gerissen hat.

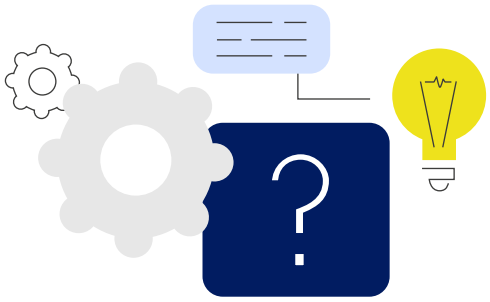
Compliance ist wie diese zusätzliche Kontrolle, die man ganz automatisch durchführt – das doppelte Abschliessen der Tür, selbst in einer ruhigen Strasse. Es ist der Entwickler, der die API-Schlüssel vorsichtshalber aktualisiert. Oder der Systemadministrator, der am Wochenende die Protokolle überprüft. Stillschweigende Gewohnheiten, die für Stabilität sorgen.

Kollektive Verantwortung

Das ist nicht nur meine Aufgabe, das ist die Aufgabe von allen. Jedes Teammitglied – nicht nur die Audit-Teilnehmenden – muss Annahmen hinterfragen, Anomalien erkennen und Risikobewusstsein über Abkürzungen stellen. Zertifizierte Unternehmen werden immer wieder angegriffen, aber wir müssen nicht die nächsten sein. Denken Sie zwei Schritte voraus und verlangen Sie für jede Behauptung Belege. Zertifikate gewinnen Kunden, aber die richtige Einstellung verhindert Verstösse.

Sprechen wir darüber

Wenn Sie das nächste Mal das Hässliche mit Fragen auf sich zukommen sehen, versuchen Sie darin einen Partner zu sehen und kein Hindernis. Fragen Sie mich nach dem «Warum». Teilen Sie mir Ihre Sichtweise mit. Gemeinsam machen wir die Dinge stärker. Denn letztendlich geht es hier nicht um Regeln. Es geht darum, dass wir das, was wir aufgebaut haben, auch für die Zukunft sichern.



Über José Francisco Agulló

José Francisco Agulló, unser Qualitätsmanager bei ERNI Spanien in Valencia, unterstützt Teams bei der Entwicklung zuverlässiger, konformer und hochwertiger Softwarelösungen in regulierten Umgebungen. Mit seinem Hintergrund in Wirtschaftsingenieurwesen und Qualitätssicherung und als ISO 27001 Lead Auditor verbindet er praktische Ingenieurserfahrung mit einem pragmatischen Ansatz in Bezug auf Risiko, Sicherheit und Qualität.

Realer Anwendungsfall für Cybersicherheit im Rahmen des EU-Gesetzes zur Cyberresilienz

Digitale Produkte entwickeln sich zu komplexen Ökosystemen, die Cloud-Dienste, eingebettete Steuerungen, mobile Anwendungen und Unternehmensintegrationen kombinieren. Deshalb steigen ihre Anforderungen an die Cybersicherheit exponentiell. Mit dem EU-Cyberresilienzgesetz und strengeren MDR-, ISO 14971- und IEC 81001-5-1-Vorschriften müssen Hersteller belegen, dass ihre Produkte während des gesamten Lebenszyklus sicher sind.

Von José Francisco Agulló, Quality Manager, ERNI Spanien

Vor kurzem hat unser Team einen Hersteller bei der Vorbereitung eines vernetzten Systems der nächsten Generation unterstützt, das Cloud-Komponenten, eingebettete Geräte, drahtlose Schnittstellen und Integrationen von Drittanbietern umfasst. Die Einzelheiten sind zwar vertraulich, doch die Herausforderungen sind repräsentativ für das, womit viele Unternehmen heute konfrontiert sind.

Dieser Artikel beschreibt, wie wir das Beratungsprogramm strukturiert haben, die Gründe für unsere Methodik und die strategischen Erkenntnisse – und zeigt, wie «Sicherheit durch Design» in der Praxis bei realen Produkten aussieht.

Warum Cybersicherheit während des gesamten Lebenszyklus nicht mehr nur optional ist

Vorschriften wie der Cyber Resilience Act verändern die Cybersicherheit grundlegend von einem Best-Effort-Ansatz zu einer gesetzlichen Verpflichtung. Die Hersteller müssen nun:

- Bedrohungen bereits in der Entwurfsphase identifizieren
- Für sichere Standardeinstellungen und Aktualisierungsmechanismen sorgen
- Eine SBOM (Software Bill of Materials) führen
- Die Nutzbarkeit vor der Markteinführung bewerten
- Prozesse zum Schwachstellenmanagement implementieren
- Sicherheitskontrollen in einer technischen Datei dokumentieren
- Die Überwachung nach der Markteinführung während des gesamten Lebenszyklus unterstützen

Für viele Unternehmen sind dies völlig neue Disziplinen. Unser Anwendungsfall konzentrierte sich auf die Erstellung eines strukturierten, vertretbaren und nachvollziehbaren Sicherheitsprogramms, das diese Verpflichtungen in klare technische Verfahren umsetzt.

Sicherheit vom Grundprinzip her aufbauen: Bedrohungsmodellierung und Risikoanalyse

Das Engagement begann dort, wo jedes sichere Produkt beginnen sollte: mit einem tiefgreifenden Verständnis des Systems und seiner Risiken.

Unsere Philosophie: Man kann nicht sichern, was man nicht versteht. Und man kann ein System nur verstehen, wenn man modelliert, wie Daten durch dieses System fliessen. Darum haben wir mit den Ingenieurteams Folgendes erstellt:

- Datenflussdiagramme der Stufen 0 und 1
- Vertrauensgrenzen für Cloud-, Embedded-, Mobil- und Unternehmensschnittstellen
- STRIDE-basierte Bedrohungsmodelle für jede Komponente
- Eine Risikomatrix gemäss MDR + CRA Artikel 10

Diese Phase erfordert Klarheit über folgende Punkte:

- Wo befinden sich sensible Daten?
- Welche Module bieten Angriffsflächen, die ausgenutzt werden können?
- In welcher Abhängigkeit stehen die Komponenten zueinander?
- Wo müssen Sicherheitskontrollen durchgeführt werden?
- Was kann schiefgehen und wie schwerwiegend sind die möglichen Folgen?

Am wichtigsten ist, dass damit die Sicherheitsabsicht festgelegt wird, die die Prüfer später in der Architektur und Dokumentation wiederfinden wollen.

Entwurf einer sicheren Architektur, die die Regulierung unterstützt

In der zweiten Phase lag der Schwerpunkt auf der Definition einer CRA-konformen Sicherheitsarchitektur. Anstatt nach der Entwicklung zusätzliche Sicherheitsebenen hinzuzufügen, war es das Ziel, diese in die Grundlage des Systems zu integrieren. Unser Ansatz folgte vier Grundprinzipien:

1. Null-Vertrauen in vernetzte Produkte

Jede Schnittstelle – Bluetooth, USB, Cloud-API, Workstation – muss standardmässig von einer Kompromittierung ausgehen.

2. Sichere Kommunikation überall

Wir haben Verschlüsselungsstrategien entwickelt für:

- **Gerät ↔ Cloud**
- **Gerät ↔ lokale Workstation**
- **Gerät ↔ Mobilgerät**
- **Firmware Update Kanäle**
- **Integrationen von Unternehmenssystemen**

3. Identität bestimmt die Autorisierung

Rollenbasierte Zugriffskontrolle und ein ordnungsgemässes IAM-Design stellen sicher, dass nur die richtigen Stellen sensible Vorgänge ausführen können. Dies ist für die Einhaltung der Vorschriften gemäss Anhang II der CRA von entscheidender Bedeutung.

4. Die Architektur muss für Prüfer nachvollziehbar sein

Das ist entscheidend: Ein sicheres System, das bei einer Prüfung nicht gerechtfertigt werden kann, ist nicht konform. Das Ergebnis war eine Spezifikation für eine sichere Architektur, die Zugriffskontrolle, Verschlüsselung, Aktualisierungsrichtlinien, sichere Standardeinstellungen und Überlegungen zur Lieferkette integriert.

Einbettung von Sicherheit in den Entwicklungslebenszyklus

Eine der grössten Lücken für Hersteller vernetzter Produkte besteht darin, dass Sicherheit häufig nicht in den SDLC integriert ist. CRA und IEC 81001-5-1 verlangen:

- Anforderungen an sichere Codierung
- Reproduzierbare Entwicklungsprozesse
- Workflows für den Umgang mit Schwachstellen
- Nachvollziehbare Nachweise für Tests und Überprüfungen
- SBOMs erstellen und pflegen

Unsere Aufgabe bestand darin, das Entwicklungsteam bei der Umsetzung dieser Konzepte zu unterstützen. Wir haben eingeführt:

- Sicherheitsanforderungen pro Modul
- SAST- und DAST-Tools
- Manuelle Überprüfungen auf sicheren Code
- Codierungsrichtlinien in Übereinstimmung mit Anhang II
- SBOM-Strategie und -Tools
- Schulungen für Entwickler zu Bedrohungsmustern und Abwehrmassnahmen

Philosophie: Sicherheit muss Teil der täglichen Entwicklungsarbeit werden – und nicht nur eine Compliance-Massnahme sein.

Validierung der Sicherheitslage durch reale Tests

Unabhängig davon, wie gut das Design auch sein mag, ein Sicherheitsprogramm ist ohne praktische Validierung unvollständig. Wir haben Folgendes durchgeführt:

- Penetrationstests über Cloud-, Geräte- und Workstation-Schnittstellen hinweg
- Fuzzing von USB- und Bluetooth-Kanälen
- Robustheitstests mit fehlerhaften Eingaben
- Protokolle, Prüfpfade und Zeitstempelintegrität validieren
- Aktualisierungsmechanismen und Rollback-Pfade überprüfen

Diese Phase dient zwei Zwecken:

- Wirksamkeit der implementierten Sicherheitskontrollen demonstrieren
- Für die technische Dokumentation der CRA erforderliche Nachweise erstellen

Die Tests deckten mehrere Bereiche mit Verbesserungspotenzial auf, bestätigten jedoch auch, dass die grundlegenden Architekturentscheidungen richtig waren.

Erstellung der technischen Unterlagen für CRA und MDR

Die Aufsichtsbehörden erwarten nicht nur Compliance, sondern auch eine nachweisbare, nachvollziehbare und überprüfbare Einhaltung der Vorschriften. Wir haben dem Kunden bei der Erstellung dieser Dokumente geholfen:

- Bedrohungsmodelle
- Schwachstellenanalysen
- Sicherheitsanforderungen
- SBOM-Dokumentation
- Aktualisierungsrichtlinie
- Risikobewertung gemäss Anhang II
- Plan zur Reaktion auf Vorfälle
- Architektur-Dossier
- Validierungs- und Testberichte

Das Endergebnis war eine vollständige, CRA-konforme technische Dokumentation, die für notifizierte Stellen und die Bewertung vor der Markteinführung bereit war.

Wichtige Erkenntnisse aus dem Fall

Dieses Engagement verdeutlicht wichtige Erkenntnisse für alle Hersteller, die vernetzte Produkte entwickeln:

1. Cybersicherheit beginnt vor der ersten Codezeile.

   Bedrohungsmodelle sparten Monate an Nacharbeit und verhinderten architektonische Fehler.

2. CRA ist nicht nur eine Regulierung, sondern ein Lebenszyklus-Mindset.

Compliance wird durch kontinuierliche Prozesse erreicht, nicht durch isolierte Ergebnisse.

3. Die Dokumentation ist genauso wichtig wie technische Kontrollen.

Prüfer müssen verstehen, warum etwas entschieden und umgesetzt wurde.

4. Sichere Entwicklung ist ein kultureller Wandel.

Teams müssen Prinzipien wie geringstmögliche Berechtigungen, tiefgreifende Verteidigung und sichere Standardeinstellungen verinnerlichen.

5. Die Tests müssen das tatsächliche Verhalten von Angreifern widerspiegeln.

Fuzz-Testing, fehlerhafte Eingaben und Endpunktmissbrauch decken Probleme auf, die herkömmliche Tests übersehen.

6. Ein strukturiertes Programm reduziert das regulatorische Risiko erheblich.

Durch ein gemeinsames Framework für Architektur, Entwicklung, Tests und Dokumentation wird Compliance überschaubar und vorhersehbar.

Fazit: Ein praktischer Weg zu sicheren, konformen und widerstandsfähigen Produkten

Das Gesetz zur Cyber-Resilienz markiert einen Wendepunkt. Hersteller vernetzter Produkte müssen nun die Sicherheit während des gesamten Lebenszyklus nachweisen – vom Entwurf über die Entwicklung und Validierung bis nach der Markteinführung. Dieser Anwendungsfall zeigt, wie ein strukturiertes Beratungsprogramm Unternehmen von Unsicherheit zu Bereitschaft führen kann:

- **Klares Verständnis der Bedrohungen**
- **Sichere Architektur**
- **Sichere Codierungspraktiken**
- **Tests, die reale Bedrohungen spiegeln**
- **Dokumentation, die behördlichen Kontrollen standhält**

Unternehmen, die Cybersicherheit als eine Ingenieursdisziplin und nicht als eine reine Checklistenaufgabe betrachten, können Produkte entwickeln, die nicht nur innovativ, sondern auch vertrauenswürdig, widerstandsfähig und mit den neuen europäischen Standards konform sind.

Über José Francisco Agulló

José Francisco Agulló, unser Qualitätsmanager bei ERNI Spanien in Valencia, unterstützt Teams bei der Entwicklung zuverlässiger, konformer und hochwertiger Softwarelösungen in regulierten Umgebungen. Mit seinem Hintergrund in Wirtschaftsingenieurwesen und Qualitätssicherung und als ISO 27001 Lead Auditor verbindet er praktische Ingenieurserfahrung mit einem pragmatischen Ansatz in Bezug auf Risiko, Sicherheit und Qualität.

Das Böse: Der Alltag eines Pentesters – Dinge kaputt machen, damit andere sie reparieren können

Pentesting beginnt selten mit Alarmmeldungen. Es beginnt mit einer stillen Anfrage, um Annahmen zu überprüfen. Dieser Artikel gibt einen Einblick in eine offensive Sicherheitsmassnahme, bei der Disziplin auf Intuition trifft, logische Fehler wichtiger sind als Exploits und echte Sicherheit dadurch entsteht, dass man nachweist, was kaputt gehen kann. Er zeigt, warum dies wichtiger ist als Richtlinien allein.

Von Iván Martínez, Software Developer und Pentester, ERNI Spanien

Die Anfrage kommt ohne grosses Drama. Keine Alarmsignale. Keine roten Warnleuchten. Nur eine E-Mail. Meist kurz. Höflich. Ein Umfang. Ein Termin. Eine Erinnerung an die Regeln der Zusammenarbeit. Manchmal nur eine Zeile wie «Wir möchten wissen, wie schlimm es wirklich ist.»

Dann lächle ich. Nicht, weil ich Chaos um seiner selbst willen geniesse, sondern weil dies der Moment ist, in dem Theorie und Realität aufeinandertreffen. Irgendwo hat jemand beschlossen, Annahmen nicht mehr blind zu vertrauen, sondern sie zu überprüfen. Und diese Entscheidung ist mehr als jede Firewall oder Richtlinie, nämlich der erste echte Schritt zur Sicherheit.

Der Ruf nach dem Bruch

Eine Anfrage für einen Penetrationstest bedeutet für mich zunächst Verantwortung. Das ist kein Spiel, auch wenn die Tools für Laien manchmal wie Spielzeuge aussehen. Es handelt sich um echte Systeme. Echte Daten. Echte Reputation. Meine Aufgabe ist es nicht, zu zeigen, wie clever ich bin, sondern zu zeigen, wie fragil Gewissheit sein kann.

Ich habe den Umfang sorgfältig gelesen. Was innerhalb der Grenzen liegt ist genauso wichtig wie das, was ausserhalb liegt. IP-Bereiche. Anwendungen. Umgebungen. Anmeldedaten oder deren Fehlen. Schwarze Box, graue Box, weisse Box. Jede Entscheidung prägt die Geschichte, die sich daraus entwickelt.

Methodik steht an erster Stelle. Immer. Bevor ich ein einziges System anfasse, richte ich mich nach einem Rahmenwerk: OWASP Testing Guide, PTES, manchmal auch MITRE ATT&CK, um Taktiken und Techniken abzubilden. Das ist keine Improvisation. Das ist Disziplin. So stelle ich sicher, dass alles, was ich finde, erklärt, reproduziert und – was am wichtigsten ist – behoben werden kann.

Erkundung: Die Landschaft kennenlernen

Die erste Phase verläuft ruhig. Keine Exploits. Keine Payloads. Nur beobachten. Erfassen. Hinhören.

Ich erkunde die Angriffsfläche wie ein Fremder, der durch eine neue Stadt spaziert, und notiere mir, welche Türen verschlossen sind, welche Fenster offenstehen und welche Lichter nachts brennen. DNS-Einträge enthüllen vergessene Subdomains. Offene Ports verraten Dienste, die schon vor Jahren hätten abgeschaltet werden sollen. Fehlermeldungen verraten weit mehr, als sie sollten.

Diese Phase ist fast meditativ. Ruhig. Es geht darum zu verstehen, wie sich das System der Welt präsentiert und wie viel es preisgibt, ohne dass man fragt. Ich dokumentiere alles. Screenshots. Versionen. Zeitstempel. Später wird jedes Detail wichtig sein.

Der erste Schub

Ausbeutung beginnt nie mit roher Gewalt. Sie beginnt mit einem Gefühl. Eine Pause, die etwas zu lang ist. Eine Antwort, die nicht ganz mit der erwarteten Logik übereinstimmt. Ein Endpunkt, der isoliert betrachtet korrekt funktioniert, aber seltsam reagiert, wenn er mit einem anderen verkettet wird. Das ist der Teil, der jemandem ausserhalb des Fachgebiets am schwersten zu erklären ist: Manchmal sieht man die Schwachstelle nicht, man spürt sie nur.

Bewusst werde ich langsamer. Hier übernimmt die Mustererkennung. Jahrelange fehlerhafte Systeme flüstern mir im Hinterkopf zu. Ich spiele den Ablauf der Anwendung in meinem Kopf noch einmal durch, nicht als Code, sondern als Absicht. Was die Entwickler damit bezwecken wollten. Wo Vertrauen den Besitzer wechselt. Wo Annahmen getroffen werden.

Ein Parameter verhält sich zu grosszügig. Ein Zustandsübergang überspringt einen Schritt. Die Authentifizierung funktioniert, aber die Autorisierung folgt einer völlig anderen Logik.

Das sind keine Schwachstellen, wie sie aus Lehrbüchern bekannt sind. Es handelt sich um Persönlichkeitsmerkmale dieses spezifischen Systems. Und genau das macht sie so gefährlich.

Zunächst teste ich vorsichtig, indem ich die Logik eher sanft anstupse, anstatt sie zu zerstören. Aus einer Anfrage werden zwei. Aus zwei wird eine Sequenz. Jede Antwort zeigt mir, ob ich mich dem Ziel nähere oder mich davon entferne. Wenn das System anders reagiert als es sollte, spüre ich das sofort. Nicht als Aufregung, sondern als Klarheit.

Dies ist der gefährliche Moment. Die Grenze zwischen kontrollierten Tests und tatsächlichen Schäden ist schmal. Jede Nutzlast wird sorgfältig vorbereitet. Jeder Schritt ist reversibel. Ich nutze Schwachstellen nicht aus, um zu dominieren – ich nutze sie, um zu verstehen.

Manchmal lädt mich das System dazu ein, tiefer einzutauchen. Eine Rolle, die niemals dazu gedacht war, eingeschränkt zu sein, wird zu einem Sprungbrett. Ein Symbol, das für einen bestimmten Kontext gedacht war, funktioniert plötzlich in einem anderen. Privilegien häufen sich nicht aufgrund eines Fehlers, sondern aufgrund einer Geschichte, die niemand zu Ende geschrieben hat. Hier offenbaren sich logische Fehler: einzigartig, nirgendwo sonst wiederholbar, entstanden aus Geschäftsregeln und nicht aus schlechtem Code. Innerhalb des Systems spüre ich das ganze Gewicht von fehlgeleitetem Vertrauen.

Innerhalb der Mauern

Sobald man drinnen ist, gibt es einen Moment, in dem alles still wird. In diesem Moment ist Disziplin am wichtigsten.

Es gibt Adrenalin, ja, aber es wird durch Zurückhaltung gemildert. Ich leere keine Datenbanken. Ich verändere keine Datensätze. Ich nehme nur die minimalen Beweise, die erforderlich sind, um die Auswirkungen zu demonstrieren, und nicht mehr. Einen Screenshot. Ein Abfrageergebnis. Eine kontrollierte Aktion, die die Reichweite ohne Schaden zeigt.

Ich denke an die Entwickler, die dieses System aufgebaut haben. An den Druck, unter dem sie standen. An die Kompromisse, die sie eingehen mussten. Die meisten logischen Fehler entstehen nicht aus Inkompetenz – sie entstehen aus Komplexität.

Und ich denke darüber nach, was dieser Zugriff über die technische Ebene hinaus bedeutet. Regulatorische Risiken. Geschäftskontinuität. Vertrauen. Das ist nicht nur eine Schwachstelle – es ist eine Risikobeschreibung. Und meine Aufgabe ist es, diese genau zu vermitteln.

Dokumentation: Erkenntnisse in Massnahmen umsetzen

Das Penetrationstesten endet nicht mit dem Erlangen des Zugriffs. Es endet, wenn Verständnis weitergegeben wurde.

Ich dokumentiere jede Erkenntnis als eine Geschichte mit einem Anfang, einer Mitte und einer Konsequenz. Nicht nur, was kaputt ist, sondern auch, warum es in diesem System kaputt geht und unter welchen Annahmen es ausnutzbar wird. Ich beschreibe den Angriffspfad in menschlichen Begriffen und ordne technische Schritte der Geschäftslogik zu.

Empfehlungen sind hier wichtig. Allgemeine Ratschläge helfen niemandem. Jede Lösung ist kontextabhängig: Vertrauensgrenzen verschärfen, Zustandsvalidierung durchsetzen, Rollen trennen, die sich niemals überschneiden sollten, serverseitige Überprüfungen hinzufügen, wo zuvor clientseitige Annahmen galten. Ich erkläre nicht nur, wie man das Problem behebt, sondern auch, wie man verhindert, dass es erneut auftritt.

Und ich denke immer schon an den erneuten Test. Eine Fehlerbehebung ist erst dann wirklich abgeschlossen, wenn sie überprüft wurde. Ich skizziere, wie der Erfolg aussehen sollte: Welche Pfade müssen nun fehlschlagen, welche Reaktionen sollten sich ändern, welche Annahmen sollten nicht mehr gelten? Ein guter erneuter Test bestätigt nicht nur den Abschluss, er stellt auch das Vertrauen wieder her.

Die Schwere wird sorgfältig anhand der Auswirkungen und der Wahrscheinlichkeit und nicht anhand der Dramatik bewertet. Ein kritisches Problem in einem Labor ist nicht dasselbe wie ein mittleres Problem in der Produktion. Der Kontext ist entscheidend. Der Bericht ist keine Trophäe. Er ist eine Landkarte.

Nachdem sich der Staub gelegt hat

Wenn der Einsatz beendet ist, gibt es keinen Triumphzug. Ich nehme an der Nachbesprechung teil. Ich beantworte Fragen und erkläre, welche Wege eingeschlagen und welche vermieden wurden. Manchmal sehe ich Erleichterung. Manchmal Ungläubigkeit. Oft Dankbarkeit.

Und dann mache ich weiter. Ein anderes System. Ein anderer Bereich. Eine weitere stille E-Mail. Ich bleibe nicht, um die Korrekturen zu beobachten. Das ist nicht meine Aufgabe. Aber ich weiss, dass irgendwo die Abwehrmassnahmen verbessert werden, weil ich gezeigt habe, wie sie versagen können.

Warum ich das mache

Mein Lebensraum ist der unangenehme Bereich zwischen Vertrauen und Beweis. Ich spüre die Spannung, die mit der Aufforderung zum Angriff einhergeht, und die Verantwortung, die damit verbunden ist. Ich geniesse die Herausforderung, ja, aber ich respektiere die Risiken noch viel mehr.

Ohne offensive Sicherheit ist Schutz nur Theorie. Eine Annahme. Ungetestet. Mit ihr wird Sicherheit real.

Über Iván Martínez

Iván Martínez, Softwareentwickler und Pentester bei ERNI Spanien, arbeitet an MedTech-Projekten im Bereich Biotechnologie und Gesundheitswesen. Er ist spezialisiert auf die Entwicklung und Optimierung von Treibern für Point-of-Care-Diagnosegeräte, die eine nahtlose Integration in Laborinformationssysteme unter Verwendung von Standards wie HL7 und ASTM ermöglichen. Angetrieben von seiner Neugierde verbindet er Softwareentwicklung mit einem starken Interesse an Cybersicherheit und sicherem Systemdesign.

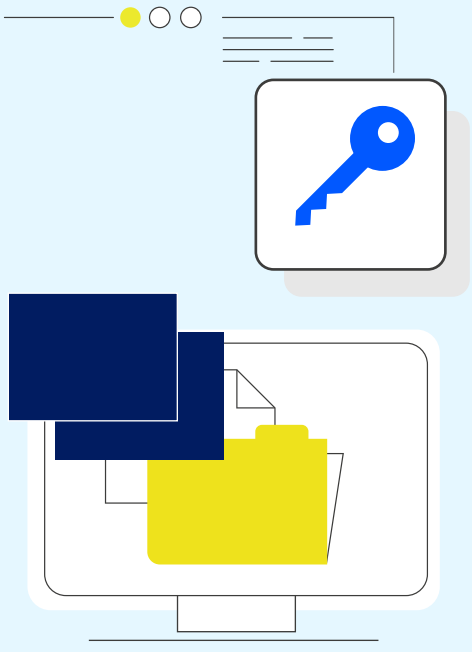
Sicherheit zum Leben erwecken: Eine Reise durch die reale Welt der Penetrationstests

Moderne vernetzte Systeme verbinden zunehmend Cloud-Dienste, mobile Anwendungen, drahtlose Protokolle und eingebettete Hardware zu einem einzigen operativen Ökosystem. Diese Konvergenz erweitert die Funktionalität, vergrössert aber die Angriffsfläche erheblich.

Von Alessandro Palermo, Senior Consultant, Program Manager und Product Owner, ERNI Schweiz

Im Rahmen eines kürzlich durchgeführten Cybersicherheitsprojekts wurde unser Team gebeten, die Sicherheitslage eines mehrschichtigen digitalen Zugangssystems zu bewerten, das in industriellen und kommerziellen Umgebungen eingesetzt wird. Details über den Kunden bleiben vertraulich. Das System kombiniert:

- Eine Cloud-Plattform zur Verwaltung von Benutzerrollen, Berechtigungen und Protokollen
- Eine mobile Anwendung, die von Technikern und Betreibern genutzt wird
- Ein IoT-Gateway, das die Konnektivität der Geräte ermöglicht
- Eine Hardware-Steuereinheit, die über den CAN-Bus kommuniziert
- Bluetooth Low Energy (BLE) für die lokale Interaktion



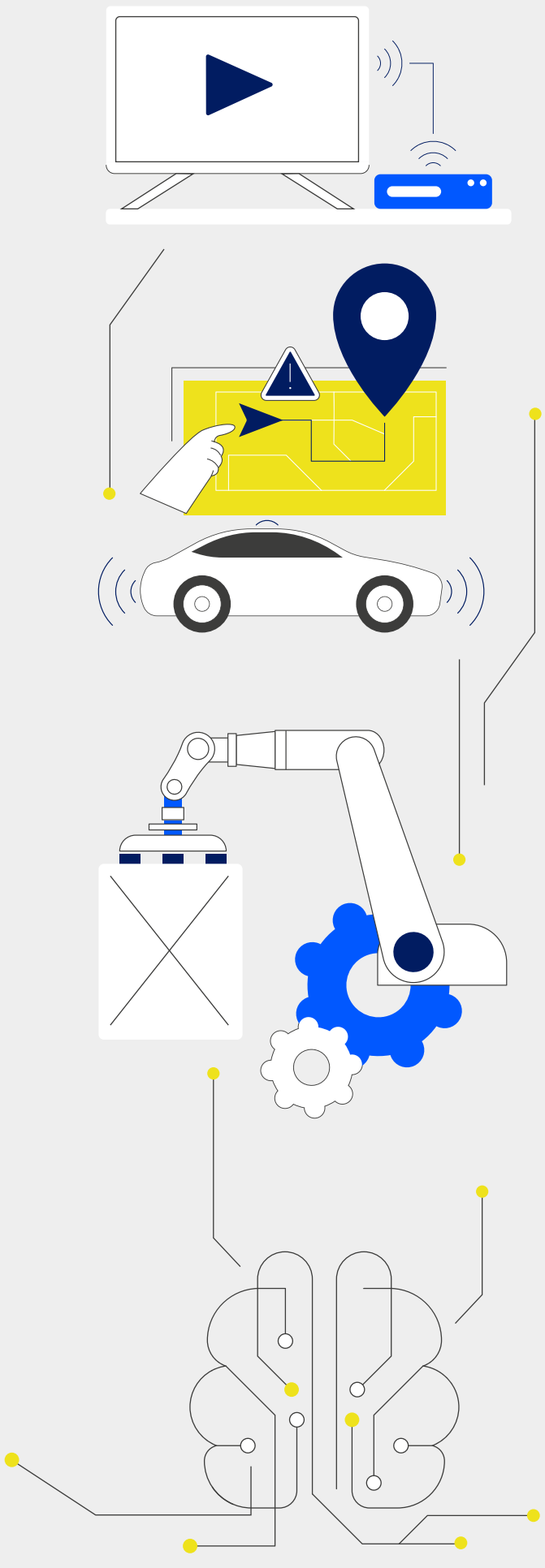
Die Herausforderung war klar: Wie bewertet man die Sicherheit eines Systems, bei dem die Cloud-Logik direkten Einfluss auf physische Vorgänge hat? Dieser Artikel beschreibt die Methodik, die Gründe für unsere Testphilosophie sowie die Erkenntnisse und zeigt, wie sich Penetrationstests in der Praxis parallel zu den Systemen, die sie schützen sollen, weiterentwickeln müssen.

Warum eine ganzheitliche Methodik wichtig ist

Viele Unternehmen betrachten Penetrationstests immer noch als eine Reihe isolierter Übungen: eine für die Webanwendung, eine andere für mobile Anwendungen, eine weitere für eingebettete Hardware. Moderne Bedrohungen machen jedoch nicht vor Abteilungsgrenzen Halt. Angreifer wechseln fliessend:

- von Mobilgeräten zur Cloud,
- von der Cloud zu physischen Geräten,
- von drahtlosen Kanälen zu eingebetteten Controllern.

Deshalb basiert unser Ansatz auf einem zentralen Prinzip: Sicherheit muss als System und nicht als einzelne Komponente bewertet werden. Diese Philosophie war ausschlaggebend für die Gestaltung unseres Testplans. Anstatt fünf separate Bewertungen durchzuführen, haben wir eine einzige übergreifende Methodik entwickelt, die Abhängigkeiten, Vertrauensgrenzen und potenzielle Pivot-Pfade im gesamten Ökosystem abbildet.



Phase 1:

VERSTÄNDNIS DES SYSTEMS DURCH BEDROHUNGS-MODELLIERUNG

Bevor wir zu den Tools kommen, befassen wir uns mit dem Kontext. Zu diesem Zweck haben wir strukturierte Workshops zur Bedrohungsmodellierung durchgeführt. Folgend zeigen wir, was wir in solchen Workshops identifizieren möchten:

- Primäre Assets (physischer Zugriff, Benutzeridentitäten, Betriebsprotokolle, Konfigurationsdaten)
- Bedrohungsakteure (externe Angreifer, betrügerische, böswillige Techniker, kompromittierte Mobilgeräte)
- Motivationen für Angriffe (unbefugtes Öffnen von Türen, Ausweitung von Berechtigungen, Offenlegung sensibler Daten, Störung des Betriebs)
- Kritische Vertrauensgrenzen (Cloud-zu-Gerät, Mobilgerät-zu-API, BLE-zu-Controller usw.)

Diese Phase dient als Leitfaden für den weiteren Verlauf des Projekts und beantwortet eine wichtige Frage: Wenn wir Angreifer mit realistischen Einschränkungen wären, wo würden wir zuerst zuschlagen? Das Ergebnis war eine nach Prioritäten geordnete Liste technischer Oberflächen, die Angreifer ausnutzen könnten. So konnten wir unsere Testbemühungen auf die wichtigsten Bereiche konzentrieren.

Phase 2:

TESTEN DER CLOUD-ANWENDUNG UND DER APIs

Die Cloud-Schicht ist das «Gehirn» des Systems. Sie verwaltet die Authentifizierung, Autorisierung und Orchestrierung der physischen Befehle, die an Feldgeräte gesendet werden. Unsere Tests kombinierten die OWASP Cloud-Native Application Security Top 10 mit einer szenariobasierten Bedrohungsmodellierung:

- Könnte ein nicht privilegierter Nutzer zu Administratorrechten eskalieren?
- Könnten falsch konfigurierte APIs unbefugte Steuerungsaktionen ermöglichen?
- Werden durch Fehlkonfigurationen in der Cloud sensible Betriebsdaten offengelegt?
- Könnten Schwachstellen die Fernsteuerung physischer Geräte ermöglichen?

Wir haben Folgendes angewendet:

- Injektionstests (SQL, Befehl, LDAP, XXE)
- Analyse der defekten Zugriffskontrolle
- Validierung der Absicherung (Header, CSP, CORS, TLS-Konfiguration)
- Überprüfung auf Offenlegung von Geheimnissen (z. B. API-Schlüssel, JWT-Fehler)
- Bewertung der Protokollierung und Überwachung
- Bewertung des Identitäts- und Zugriffsmanagements (IAM)
- Szenarien für den Missbrauch von Datei-Uploads

Die Philosophie dabei ist einfach: Cloud-Schwachstellen verstärken oft die physischen Auswirkungen. Ein kompromittiertes Dashboard kann gefährlicher sein als physische Manipulationen.

Phase 3:
BEWERTUNG DER MOBILEN ANWENDUNG

Die mobile App diente als primäre Betriebsschnittstelle für Techniker. Dadurch war sie sowohl ein Produktivitätswerkzeug als auch ein potenzieller Angriffsvektor.

Anhand des OWASP Mobile Security Testing Guide (MSTG) haben wir Folgendes bewertet:

- Sichere lokale Datenspeicherung
- Umgang mit Anmeldedaten und Verwaltung vertraulicher Informationen
- JWT-Validierung und Token-Integrität
- Sicherheitskontrollen zur Laufzeit (Root-/Jailbreak-Erkennung, Manipulationsschutz)
- Sicherheit der API-Interaktion
- Resistenz gegen Reverse Engineering (Code-Verschleierung, Binärhärtung)
- Abhängigkeitsanalyse und Überprüfung der Kryptografie

Unsere Leitphilosophie: Eine mobile App sollte davon ausgehen, dass das Gerät, auf dem sie ausgeführt wird, bereits kompromittiert sein könnte. Diese Denkweise deckt Probleme wie fest codierte Anmeldedaten, unzureichende Validierungsstrategien oder unsichere Sitzungsverwaltung auf.

Phase 4:
BEWERTUNG DER HARDWARE UND DER CAN-BUS-KOMMUNIKATION

Das eingebettete Steuerungssystem und der CAN-Bus bildeten das physische Rückgrat der Lösung. Im Gegensatz zu herkömmlichen IT-Diensten interagieren diese Komponenten mit Motoren, Sensoren und Aktuatoren – was bedeutet, dass Sicherheitslücken zu realen physischen Folgen führen können. Unsere Tests umfassten:

- Busverkehr und Protokollanalyse erfassen
- Nachrichten einschleusen und manipulieren
- Fuzz-Tests zur Bewertung der Widerstandsfähigkeit
- Manipulationsversuche an Gehäusen und Steckverbindungen
- DoS-Tests zum Verständnis der Fehlertoleranz
- ECU-Verhalten unter Belastung überprüfen
- Manipulationsschutzmassnahmen bewerten

Unsere Philosophie in diesem Bereich: Physikalische Systeme versagen selten dramatisch, sie versagen still und leise. Es ist unerlässlich, ihr Verhalten bei unerwarteten Eingaben zu verstehen. So konnten wir überprüfen, wie das Gerät auf Überflutung, fehlerhafte Frames und unerwartete Zustandsübergänge reagierte.

Phase 5:
ÜBERPRÜFUNG DES IOT-GATEWAYS UND DER VERBINDUNGSWEGE

Als Brücke zwischen lokaler Hardware und Remote-Cloud-Diensten erforderte das IoT-Gateway eine andere Perspektive. Wir haben uns dabei an den OSSTMM-Prinzipien orientiert und uns auf folgende Punkte konzentriert:

- Aufzählung der Netzwerkflächen
- Port- und Service-Exposure
- Gerätehärtung
- LAN- und GSM-Kommunikationsanalyse
- Protokollverhalten unter widrigen Bedingungen

Ein wesentlicher Bestandteil unserer Philosophie lautet: Ein sicheres Gateway ist unsichtbar. Durch eine angemessene Absicherung verschwindet die Angriffsfläche.

Phase 6:

TESTEN DER BLUETOOTH LOW ENERGY (BLE) KOMMUNIKATION

BLE ermöglicht eine einfache lokale Interaktion, birgt jedoch Risiken für Angriffe über Funkverbindungen. Unsere massgeschneiderte BLE-Methodik umfasste:

- Geräte durchsuchen und auflisten
- Kopplung und Authentifizierung testen
- Verschlüsselung validieren
- Replay- und Injektionsangriffe
- Signalresistenz bei Störungen testen
- Fuzz-Test von GATT-Diensten und -Eigenschaften

Unser Grundsatz in dieser Schicht: Drahtlose Funktionen müssen als öffentliche Einstiegspunkte behandelt werden, unabhängig von ihrer beabsichtigten Reichweite.

Wichtige Erkenntnisse aus der Bewertung

Obwohl die einzelnen Ergebnisse je nach System variieren, lassen sich in cyber-physischen Ökosystemen mehrere Erkenntnisse konsistent feststellen:

1. Das Zugriffsmanagement ist oft die grösste Schwachstelle.
   Fehlerhafte Rollenzuweisungen, unsichere API-Designs und unzureichende serverseitige Überprüfungen schaffen Möglichkeiten für eine Ausweitung der Berechtigungen.

2. Geheimnisse werden oft dort preisgegeben, wo Entwickler es am wenigsten erwarten.
   Fest codierte API-Schlüssel, unzureichende JWT-Validierung und ungeschützte Konfigurationsdateien sind branchenübergreifend weit verbreitet.

3. Mobilen Geräten kann nicht uneingeschränkt vertraut werden.
   Die Erkennung gerooteter Geräte, sichere lokale Speicherung und Code-Verschleierung bleiben unerlässlich.

4. Physische Geräte erfordern Ausfallsicherheit, nicht Perfektion.
   Ausfallsicheres Verhalten, Manipulationserkennung und robuste Ratenbegrenzung auf Kommunikationsbussen sind wichtiger als komplexe kryptografische Designs.

5. Überwachung und Reaktion auf Vorfälle werden oft übersehen.
   Ein System kann zwar unbefugte Zugriffe erkennen, aber ohne Alarmierung passiert nichts.

Eine Philosophie der praktischen Sicherheit entwickeln

Unsere Methodik ist nicht tool-orientiert, sondern wirkungsorientiert. In jeder Phase stellen wir folgende Fragen:

- Was sind die realen Folgen dieser Schwachstelle?
- Kann diese Schwachstelle mit realistischen Angriffsfähigkeiten ausgenutzt werden?
- Wie beeinflusst diese Komponente das Verhalten des Gesamtsystems?
- Versagt das System auf sichere oder gefährliche Weise?

Diese Perspektive ermöglicht es uns, die Testtiefe dynamisch über alle Komponenten hinweg anzupassen und so den höchsten Nutzen für den Kunden zu gewährleisten.

Fazit: Sicherheit über die Grenze zwischen digitaler und physischer Welt hinweg

Da die Industrie zunehmend auf vernetzte Geräte angewiesen ist, verschwimmt die Grenze zwischen Cybersicherheit und physischer Sicherheit immer mehr. Eine Fehlkonfiguration in der Cloud kann eine physische Tür öffnen, ein Fehler in einer mobilen App kann zu einer Ausweitung von Berechtigungen führen und eine CAN-Nachricht kann den Betrieb stören. Unser aktuelles Engagement zeigt, dass effektive Sicherheitsbewertungen Cloud-, Mobil-, IoT-, Wireless- und Embedded-Tests in eine einheitliche Methodik integrieren müssen. Unternehmen, die diese ganzheitliche Perspektive übernehmen, erhalten mehr als nur einen Schwachstellenbericht – sie gewinnen Klarheit, Widerstandsfähigkeit und Vertrauen in die Systeme, die ihren Betrieb am Laufen halten.

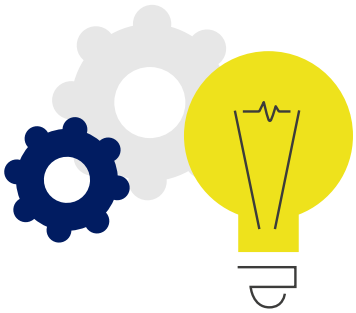
Über Alessandro Palermo

Alessandro Palermo, Senior Consultant, Programmmanager und Product Owner bei ERNI Schweiz, leitet komplexe digitale Projekte für globale Kunden. Er ist PMP-zertifiziert und spezialisiert sich auf agile Führung, Produktvision und Stakeholder-Management. Er begleitet interdisziplinäre Teams vom Konzept bis zur Markteinführung. In seiner Arbeit verbindet er Strategie und Umsetzung mit Fokus auf Kundennutzen und nachhaltige Lieferung.

Wenn sich der Staub gelegt hat: Was bleibt an der digitalen Front übrig?

In klassischen Western endet die Geschichte nicht mit dem letzten Schuss. Sie endet, sobald sich der Staub gelegt hat, wenn die Stadt über ihre Zukunft entscheidet. In der modernen Cybersicherheit ist es genauso: Es geht nicht um die Sicherheitsverletzung, die Prüfung oder die Bereitstellung – es geht darum, was danach passiert und wie Teams widerstandsfähige, sichere Systeme aufbauen.

Von David Soto Dalmau, Cybersecurity Principal, ERNI Spanien



In dieser Ausgabe haben wir uns mit komplexen Themen befasst: sichere Entwicklung, Regulierung, offensive Tests, rechtliche Rahmenbedingungen, vernetzte Systeme, physische Geräte, Cloud-Plattformen, Code, Prozesse und Menschen. Wir haben reale Bedrohungen, wachsende Verpflichtungen und Architekturen untersucht, die sich keine Naivität mehr leisten können. Wenn es jedoch eine Idee gibt, die sich durch alle Seiten zieht, dann ist es diese: Sicherheit ist kein Zustand – sondern eine Arbeitsweise.

Der Mythos vom sicheren System

Seit Jahren verfolgt die Branche still und leise ein Versprechen: Wenn wir genug tun, werden wir irgendwann einen Punkt erreichen, an dem ein System sicher ist.

Dieser Punkt existiert nicht. Nicht, weil uns Werkzeuge, Standards oder Talente fehlen, sondern weil lebende Systeme, die sich weiterentwickeln, integrieren, verbinden und skalieren, niemals statisch sind. Der Kontext ändert sich. Die Akteure werden anders. Die Anreize verschieben sich. Und vor allem wird Vertrauen auf neue Weise ausgenutzt. Reife entsteht nicht, wenn Schwachstellen verschwinden. Sie entsteht, wenn sie uns nicht mehr überraschen.

Drei Perspektiven, eine gemeinsame Verantwortung

In diesem Magazin haben wir drei Kräfte, die schon immer vorhanden waren, Gestalt und Stimme verliehen:

- Die, die mit Absicht und Disziplin aufbauen,
- Die, die Grenzen setzen, damit Lektionen nicht vergessen werden,
- Die, die Annahmen brechen, um zu beweisen, dass die Realität nicht verhandelbar ist.

Ein häufiger Fehler besteht darin, diese als getrennte Funktionen zu behandeln. Das eigentliche Risiko

entsteht, wenn sie zu Silos werden. Wenn die Entwicklung ohne Validierung voranschreitet, wird das Vertrauen brüchig. Wenn Regulierung ohne technisches Verständnis existiert, wird sie zu Lärm. Und wenn Angriffe ohne Kontext durchgeführt werden, werden sie zum Spektakel.

Wirksame Sicherheit entsteht nur, wenn diese Perspektiven sich gegenseitig herausfordern, voneinander lernen und sich gegenseitig zu Verbesserungen zwingen. Das ist nicht bequem. Aber es ist zutiefst professionell

Von der Einhaltung zur Überzeugung

Vorschriften wie der Cyber Resilience Act sind nicht das Ziel, sie sind ein Signal. Sie spiegeln, was viele Unternehmen bereits auf schmerzhafte Weise lernen mussten: Sicherheit kann nicht von vereinzelten Heldentaten oder Last-Minute-Massnahmen vor einer Prüfung abhängen.

Resiliente Organisationen zeichnen sich nicht dadurch aus, dass sie Bewertungen bestehen, sondern durch ihre Fähigkeit, klar und ehrlich zu erklären, warum ihre Systeme so konzipiert sind, wie sie sind, welche Risiken sie bewusst eingehen und wie sie reagieren werden, wenn etwas schiefgeht.

Denn etwas wird schiefgehen. Entscheidend ist nicht, ob es passiert, sondern wie gut wir darauf vorbereitet sind.

Die eigentliche Veränderung ist nicht technischer Natur

Nach all den Tools, Architekturen, Bedrohungsmodellen und Tests bleibt eine unbequeme Schlussfolgerung: Die bedeutendsten Fortschritte in der Cybersicherheit sind nicht technologischer Natur, sie sind kultureller Art. Sie finden statt, wenn:

- **Entwickler verstehen, dass Sicherheit Teil der Qualität ist,**
- **Compliance-Experten die von ihnen verwalteten Systeme verstehen,**
- **Offensive Teams als Verbündete beim Lernen angesehen werden und nicht als Überbringer schlechter Nachrichten.**

Sie finden statt, wenn sich die Diskussion weg von «Wer hat versagt?» hin zu «Was hat uns das System dieses Mal gelehrt?» bewegt.

Wenn sich der Staub gelegt hat

In Westernfilmen ist der wirklich entscheidende Moment nicht das Duell, sondern der Moment, in dem jemand erkennt, dass er seine Hand nicht mehr über seiner Waffe halten muss. In der digitalen Welt kommt dieser Moment, wenn Sicherheit nicht mehr eine ständige Reaktion ist, sondern zu einer integrierten, alltäglichen Praxis wird – fast unsichtbar.

Nicht, weil das Risiko verschwunden ist, sondern weil die Organisation gelernt hat, damit zu leben, ohne es zu leugnen.

Das ist das Ziel, auf das alles, was Sie hier gelesen haben, hinweist. Keine Welt ohne Bedrohungen, sondern eine Welt, in der wir das Spiel verstehen, seine wirklichen Regeln erkennen und Verantwortung für die Rolle übernehmen, die wir spielen. Der Staub legt sich. Das System bleibt lebendig. Und die eigentliche Arbeit – die sinnvolle Aufgabe – geht weiter.

Über David Soto Dalmau

David Soto Dalmau ist Leiter des Bereichs Cybersicherheit bei ERNI in Barcelona. Als lebenslanger Enthusiast für ethisches Hacking und Capture the Flag (CTF) kombiniert er Fachwissen in Kryptografie, Penetrationstests und Risikomanagement mit der Vermittlung und Förderung einer Kultur des kontinuierlichen Lernens.

Über ERNI

ERNI steht für Swiss Software Engineering. Woran sind wir wirklich interessiert? Wie können wir Sie und Ihre Mitarbeitenden besser als jedes andere Unternehmen bei der Entwicklung und Vermarktung softwarebasierter Produkte und Dienstleistungen unterstützen? Unsere globale Plattform für Softwareentwicklung in Kombination mit einem fundierten Marktverständnis bildet den Rahmen für den Erfolg unserer Kunden. Unser Team implementiert auch komplexe Projekte, befähigt Menschen und liefert herausragende Kundenlösungen in kürzester Zeit. Wir wenden die Schweizer Mentalität mit Verhaltensmustern wie Konsensbildung, Pragmatismus, Integration, Zuverlässigkeit und Transparenz auf globaler Ebene an – und dies seit unserer Gründung im Jahr 1994; zusammen mit unserem grossartigen Team, das die Basis für Ihre erfolgreichen Software-Projekte ist. Heute beschäftigt die ERNI Group weltweit mehr als 800 Mitarbeitende.

Über .experience

In diesem Magazin, das von ERNI mehrmals im Jahr veröffentlicht wird, informieren wir über wichtige Erfahrungen, die wir bei unserer täglichen Arbeit in den Bereichen Zusammenarbeit, Prozesse und Technologie machen.

Impressum

Ausgabe 1/2026

ERNI

Swiss Software Engineering
betterask.erni

Herausgeber

ERNI Management Services AG

ERNI Standorte

ERNI Schweiz AG
Bern
Zürich
Luzern
Lausanne
Basel

ERNI Consulting España S.L.U.
Barcelona
Madrid
Sant C. del Vallès

ERNI Development Center Spain, S.L.
Valencia

ERNI (Germany) GmbH
Frankfurt
München
Berlin
Stuttgart

ERNI Development Center Philippines Inc.
Manila

ERNI Development Center Romania S.R.L.
Cluj-Napoca

ERNI Singapore PTE. LTD.
Singapur

ERNI (Slovakia) s.r.o.
Bratislava

ERNI USA
New York

Kontakt

ERNI Management Services AG
Löwenstrasse 11 I 8001 Zürich
Email: marketing@betterask.erni
Phone: +41 58 268 12 00
Web: www.betterask.erni

ERNI in den Social Media Netzwerken