



swisscom

EINE SUCCESS STORY

WIE SWISSCOM 400.000 USD EINSPART

Pro vermiedenem IoT-Sicherheitsvorfall
durch automatisierte Firmware-Analyse

BAHNBRECHENDE IOT-FIRMWARE-SICHERHEIT ALS SCHLÜSSEL ZU SERVICEQUALITÄT, LIEFERANTENBEZIEHUNGEN UND MARKENREPUTATION

Zusammenfassung

Swisscom analysiert mit **ONEKEY** +80 Firmware-Images pro Jahr, hauptsächlich während des Kaufprozesses für neue IoT-Geräte, aber auch in der kontinuierlichen Entwicklung und im Support. Somit erzielt Swisscom einen Sicherheits-ROI von bis zu 374.000 CHF pro vermiedenen Firmware-Rollout:

- Software Security Quality Gate: Verbesserung der IoT-Sicherheit und Stärkung der Verhandlungsposition gegenüber Geräteherstellern dank automatisierter Sicherheitsanalysen und Compliance-Prüfungen, die von Herstellern häufig vernachlässigt werden.
- Minimierung der Reparatur- und Wartungskosten durch systematische Identifizierung kritischer Sicherheitslücken vor der Einführung neuer Firmware.
- Gewährleistung von erstklassigem Service und Markenimage durch Einhaltung der höchsten Sicherheitsstandards für Geräte vor Ort beim Kunden.

Vorreiter auch in Zeiten erhöhter Komplexität

Swisscom ist das führende Telekommunikationsunternehmen der Schweiz und einer der größten IT-Dienstleister des Landes mit einem Marktanteil von über 60% in den Bereichen Mobil- und Breitband und einem Gesamtumsatz von 11,2 Mrd. CHF (2021).

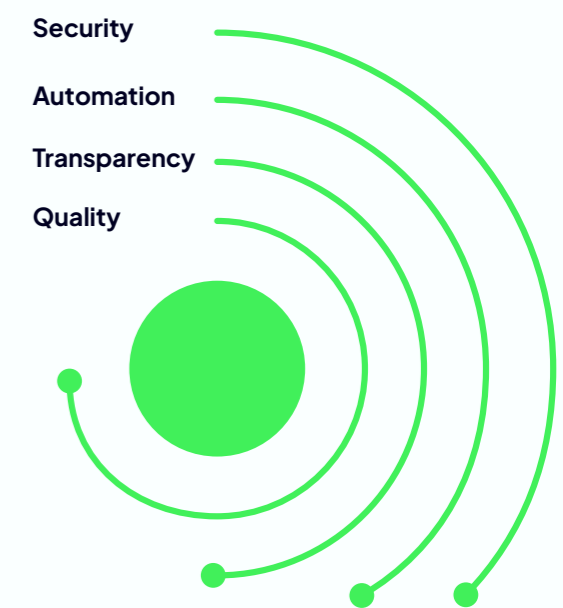
Seit über einem Jahrhundert ist Swisscom das Qualitätsportal für Telekommunikationsprodukte auf dem Schweizer Markt. Dank der Firmware-Analysekapazitäten von ONEKEY führt Swisscom Tests durch, die zuvor von



den Herstellern vernachlässigt wurden, und behauptet damit ihre Vorreiterrolle, auch wenn die Gerätesicherheit immer komplexer wird.

Swisscom begann vor Jahren mit **ONEKEY** zu arbeiten. Als das Telekommunikationsunternehmen die Plattform zum ersten Mal implementierte, konzentrierte es sich hauptsächlich auf die Analyse von kundeneigenen Geräten (CPE), die für seine Privat- und KMU-Kunden konzipiert waren.

Da Hersteller von IoT-Geräten mit kurzen Produktlebenszyklen, starkem Wettbewerb, komplexen Lieferketten und einer intensiven Konzentration auf sich ständig weiterentwickelnde Produktmerkmale zu kämpfen haben, ist die Sicherheit oft unzureichend.



11.2B

60%



Transparenz in undurchsichtige Lieferketten bringen

ONEKEY dient als Qualitäts-Gateway für CPE – sei es für Privat- und KMU-Kunden – wie Wi-Fi-Router und Repeater, Hotspots und andere Geräte, die in fast jedem Heim- oder Firmenbüro in der Schweiz zu finden sind.

ONEKEY ist nahtlos in den Entwicklungsprozess von Swisscom integriert, wo die systematische Analyse von +80 Firmware-Images pro Jahr zu einer erhöhten Sichtbarkeit der Lieferkette führt. Die detaillierten Firmware-Sicherheits- und Compliance-Analysen von ONEKEY er-



“**ONEKEY** hilft uns erheblich bei der Entwicklung und dem Betrieb von Geräten vor Ort beim Kunden. Wenn wir überprüfen, ob sich die Software im Status „Release Candidate“ befindet, können wir potenzielle sicherheitsrelevante Fehler früher erkennen und sie dem Lieferanten zur Korrektur oder Analyse melden. Die Bewertung der einzelnen Module und Plugins in ONEKEY ermöglicht es uns, risikobasierte Entscheidungen zu treffen, wenn wir über neue Funktionen oder Schnittstellen verhandeln.”

– Giulio Grazi, Senior Security Consultant, Swisscom



möglichen es Swisscom, gut auf Verhandlungen mit Geräteanbietern und Herstellern vorbereitet zu sein, und ermöglichen es dem Telekommunikationsunternehmen, fundierte und faktengestützte Diskussionen mit Lieferanten zu führen. Swisscom bietet ihren Anbietern den Mehrwert bisher unbekannter Sicherheitsprobleme, die von ONEKEY identifiziert wurden, und hat sich damit in eine einzigartige Position gebracht. Swisscom und ihre Anbieter haben eng zusammengearbeitet, um das Sicherheitsniveau der Geräte vor Ort beim Kunden kontinuierlich zu erhöhen.

Swisscom spart 374.000 CHF pro vermiedenem Vorfall

Bei rund 1,8 Millionen Geräten im Einsatz hinterlässt jedes von Swisscom implementierte Firmware-Upgrade einen großen Support-Fußabdruck. Für einen winzigen Prozentsatz der Geräte, die nicht erfolgreich aktualisiert werden (z. B. weil das Gerät während des Vorgangs die Stromversorgung verloren hat), werden Support-Techniker zu den Kunden geschickt, um Geräte zu reparieren oder auszutauschen. Im Durchschnitt kostet jedes Firmware-Upgrade geschätzte CHF 374.000 an Support.

Daher ist es von größter Bedeutung, dass jedes Upgrade frei von kritischen (und vermeidbaren!) Sicherheitslücken. Jedes auftretende Problem kann es erforderlich machen, kurz nach der vorherigen Version ein neues Upgrade herauszugeben. Indem kritische Sicherheits- und Konfigurationsprobleme hervorgehoben werden, **ONEKEY** trägt erfolgreich zu diesem Ziel bei. Indem nur ein einziges fehlerhaftes Upgrade (und die anschließende Notwendigkeit, es zu beheben) verhindert wird, **ONEKEY** trägt bereits zu einem Sicherheits-ROI von CHF 374.000 bei. Fast zur gleichen Zeit als **ONEKEY** integriert wurde, lancierte Swisscom ihr Bug-Bounty-Programm. Dank der gründlichen internen Firmware-Sicherheitsanalyse – und dem damit erhöhten Sicherheitsniveau ihrer Produkte – ist die Qualität der eingereichten IoT-Bugs kontinuierlich hoch geblieben, sodass Bug-Hunter nicht in der Lage waren, sich die mögliche Sicherheitslücken zu schnappen.



75% | der Unternehmen wünschen sich eine SBOM für alle Softwareprodukte.*



37% | der Unternehmen hatten bereits einen IoT-bezogenen Sicherheitsvorfall.*

INTEGRATION DER IOT-FIRMWARE- SICHERHEIT IN NEUE GESCHÄFTSMODELLE

Aufgrund des Erfolgs in ihren Privat- und KMU-Geschäftsbereichen beschloss Swisscom, den Einsatz von **ONEKEY** in neue Bereiche auszuweiten. Das Telekommunikationsunternehmen konzentriert sich zunehmend auf umfassende IoT-Lösungen für seine Industriekunden. Konnektivität für IoT-Ökosysteme sowie IoT-Gateways und IoT-Managementlösungen stehen im Mittelpunkt dieser neuen Serviceangebote. Während des gesamten Entwurfs, der Erstellung und der laufenden Wartung des Dienstes **ONEKEY** hat als Qualitäts-Gateway für die Auswahl, Implementierung und Veröffentlichung von Geräten sowie für die kontinuierliche Überwachung neuer Sicherheitsbedrohungen eine wichtige Rolle gespielt und es Swisscom ermöglicht, ihren IoT-Dienst auf einem sicheren Stack aufzubauen.

Das jüngste Beispiel für einen solchen Service ist das „Gateway as a Service“-Angebot von Swisscom, bei dem das Telekommunikationsunternehmen Wi-Fi- oder Ethernet-Gateways und Konnektivität für die IoT-Ökosysteme der Pharma- und Fertigungsbranche bereitstellt. Mit diesem neuen Service können Hersteller von Barista-Kaffeemaschinen nun bequem auf ihre Geräte zugreifen, um Fernsupport und vorausschauende Wartung durchzuführen. Und Seilbahnanbieter, die Informationsplattformen an weit entfernten Orten betreiben, können ihre Geräte aus der Ferne verwalten, ohne unwirtliches Gelände bereisen zu müssen. Für den Betrieb an solch zentralen und exponierten Standorten sowie für die Verbindung sensibler und geschäftskritischer Prozesse müssen die Gateways äußerst sicher sein. **ONEKEY** ist die Lösung der Wahl, da sie einfach und transparent bewertet und als digital-twin überwacht werden können.

ÜBER ONEKEY

ONEKEY ist ein führender europäischer Spezialist für automatisierte Sicherheits- und Compliance-Analysen für Geräte in den Bereichen Fertigung (OT) und Internet der Dinge (IoT). Mithilfe der automatisch generierten „digitalen Zwillinge“ und der „Software-Stückliste (SBOM)“ von Geräten analysiert ONEKEY eigenständig die Firmware auf kritische Sicherheitslücken und Compliance-Verstöße – und das alles ohne Quellcode-, Geräte- oder Netzwerkzugriff.

Schwachstellen für Angriffe und Sicherheitsrisiken werden in kürzester Zeit identifiziert und können so gezielt behoben werden.

Die Lösung lässt sich leicht in Softwareentwicklungs- und Beschaffungsprozesse integrieren und ermöglicht es Herstellern, Händlern und Nutzern der IoT-Technologie, Sicherheit und Konformität schnell und automatisch vor der Verwendung und rund um die Uhr während des gesamten Produktlebenszyklus zu überprüfen.

Führende Unternehmen wie SNAP ONE, SWISSCOM, TRIMBLE, VERBUND AG, ZYXEL und viele andere profitieren heute von dieser Plattform – Universitäten und Forschungseinrichtungen können die ONEKEY-Plattform kostenlos für Studienzwecke nutzen.



onekey.com
+49 211 1587 41 04
info@onekey.com



© 2022 ONEKEY. Alle Rechte vorbehalten. Vervielfältigung nur mit Genehmigung von ONEKEY gestattet. Alle aufgeführten Marken sind die Marken der jeweiligen Eigentümer. Irrtümer, Änderungen und Verfügbarkeiten der aufgeführten Produkte, Dienstleistungen, Eigenschaften und Anwendungsmöglichkeiten bleiben vorbehalten. ONEKEY übernimmt keine Gewähr für Auskünfte Dritter über Eigenschaften, Leistungen und Verwendbarkeit. ONEKEY behält sich vor, Produkte und Leistungen im Rahmen der Produktentwicklung auch ohne vorherige Ankündigung zu ändern. Bei Abweichungen von den Vertragsunterlagen und Allgemeinen Geschäftsbedingungen von ONEKEY und deren verbundenen Unternehmen und Tochtergesellschaften in Verbindung mit diesem Dokument haben die Vertragsunterlagen und Allgemeinen Geschäftsbedingungen stets Vorrang vor diesem Dokument.