NIS2 KONFORM CYBER SECURITY

SICHERE ENTWICKLUNG LEBENSZYKLUSPROZESS

Honeywell hat ein robustes System entwickelt, um Sicherheit zu Beginn der Produktkonzeption und während der Entwicklung zu berücksichtigen und auf potenzielle Schwachstellen in bestehenden Produkten zu reagieren. Dieses System, die SSDLC - Secure Software Development Lifecycle-Initiative von Honeywell, hat sich in den letzten Jahren weiterentwickelt und ist noch robuster geworden.

Honeywell nimmt Produktsicherheit ernst. Unsere Produkte durchlaufen ein robustes und umfassendes Penetrationstestprogramm.
In einigen Fällen werden zusätzliche unabhängige Sicherheitstests durchgeführt. Die Kriterien für diese zusätzlichen Tests sowie die dafür ausgewählten Produkte oder Angebote sind vertrauliche Informationen.

Wir verfügen über einen robusten und umfassenden Entwicklungslebenszyklus (SDLC) basierend auf Best Practices und Industriestandards und dieser umfasst Folgendes:

- Sicherheitsrisikobewertung basierend auf Bedrohungsumfeld, dem ein bestimmtes Produkt oder Angebot ausgesetzt ist, sowie die technischen Merkmale und Kundenbedürfnisse
- Sicherheitsanforderungen und Sicherheit Kontrollen basierend auf Industriestandards und Richtlinien wie BSIMM, ISA/IEC 99/62443, ISO 27001, PCI DSS, DSGVO, OWASP, geltende lokale Gesetze und Vorschriften und andere, abhängig vom Produkt oder Angebot und dem Sicherheitsrisiko Bewertung
- Datenschutz-Folgenabschätzungen
- Bedrohungsmodellierung
- Sicher durch Design, Datenschutz durch Design und Sichere Codierungsstandards und -praktiken
- Statische Anwendungssicherheitstests (SAST, auch bekannt als Quellcode-Scanning) zur Durchsetzung sicherer Design- und Codierungspraktiken. Wir scannen nach OWASP-Top-10- und SANS-Top-25-Schwachstellen sowie nach sprachspezifischen Qualitätsmaßstäben. Zu den aktuellen SAST- Tools gehören je nach Produkt- und Sprachanforderungen SonarQube und Coverity
- Binäres Scannen zur Identifizierung der Open-Source-Nutzung und potenzieller Schwachstellen
- Eine formelle Risikomanagementrichtlinie, die spezifische Zeitpläne zur Risikominderung je nach Schweregrad vorschreibt
- Überprüfung und Genehmigung der Cybersicherheit durch leitende Angestellte vor dem Versand des Produkts
- Lebenszyklus-Support und Kunden-benachrichtigung für Sicherheitsupdates

Ein Audit-Team von Honeywell führt Kontrollen durch, um sicherzustellen, dass die im Rahmen der Honeywell-Prozesse des sicheren Entwicklungslebenszyklus erforderlichen Sicherheitsleistungen erbracht werden. Honeywell führt für seine Mitarbeiter Schulungsprogramme zu den Sicherheitsprozessen des Unternehmens sowie zu spezifischen Problemen und Lösungen im Bereich der Cybersicherheit durch.

Alle Softwareentwickler bei Honeywell erhalten eine formelle Schulung zum Secure Development Life Cycle-Prozess und zu allgemeinen Cyber-/Produktsicherheitsthemen.

NETZWERK UND INFORMATIONSSICHERHEIT RICHTLINIE 2 (NIS2)

Richtlinie (EU) 2022/2555 des Europäisches Parlament und des Rat vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Maß an Cybersicherheit in der gesamten EU Union, Änderungsverordnung (EU) Nr. 910/2014 und Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS2-Richtlinie)

Die 2016 durch die NIS-Richtlinie eingeführten EU-Cybersicherheitsanforderungen wurden durch die NIS2-Richtlinie, die 2023 in Kraft trat, aktualisiert und gestärkt. Angesichts der zunehmenden Digitalisierung mit zunehmenden Cyberangriffen und einer sich insgesamt entwickelnden Cybersicherheitsbedrohungs-landschaft hat die EU strengere Aufsichtsvorschriften eingeführt Maßnahmen mit Kapazitäten zur Reaktion auf Vorfälle und strengeren Durchsetzungsanforderungen durch Ausweitung auf neue Sektoren und Einheiten.

Bis zum 17. Oktober 2024 müssen alle EU-Mitgliedsländer die zur Einhaltung der NIS2-Richtlinie erforderlichen Maßnahmen verabschieden und veröffentlichen und diese Maßnahmen ab dem 18. Oktober 2024 anwenden.

Honeywell

HONEYWELL CYBERSECURITY REPORTING POLITIK

Das Ziel unseres Product Security Incident Response Teams (PSIRT) besteht darin, das mit Sicherheitslücken verbundene Risiko für Kunden zu minimieren, indem wir rechtzeitig Informationen, Anleitung und Behebung von Schwachstellen in unseren Produkten, einschließlich Software und Anwendungen, Hardware und Geräten, Diensten und Lösungen, bereitstellen. Dieses Team verwaltet den Empfang, die Untersuchung, die interne Koordination, die Behebung und die Offenlegung von Informationen zu Sicherheitslücken im Zusammenhang mit Honeywell-Produkten.

PSIRT koordiniert die Reaktion und Offenlegung aller extern identifizierten Produktschwachstellen.

MELDUNG EINER POTENZIELLEN SICHERHEITSLÜCKE

Wir freuen uns über Berichte von unabhängigen Forschern, Branchenorganisationen, Anbietern und Kunden, die sich mit Produktsicherheit befassen. Weitere Informationen zum Melden einer potenziellen Sicherheitslücke finden Sie auf der Webseite zur Meldung von Sicherheitslücken unter https://www.honeywell.com/us/en/product-security#vulnerability-reporting

KOORDINIERTE OFFENLEGUNG VON SCHWACHSTELLEN (CVD)

Wir sind bestrebt, die Coordinated Vulnerability Disclosure (CVD) einzuhalten. Dieser Prozess ermöglicht es unabhängigen Reportern, die eine Schwachstelle entdecken, direkt mit Honeywell Kontakt aufzunehmen und gibt uns die Möglichkeit, die Schwachstelle zu untersuchen und zu beheben, bevor der Reporter die Informationen der Öffentlichkeit preisgibt.

Das PSIRT wird sich während der gesamten Schwachstellenuntersuchung mit dem Meldenden abstimmen und ihn gegebenenfalls über den Fortschritt informieren.
Mit ihrer Zustimmung kann das PSIRT den Meldenden in unseren Danksagungen für das Auffinden einer gültigen Produktschwachstelle und die private Meldung des Problems erwähnen. Nachdem Honeywell eine Aktualisierung oder Schadensbegrenzungsinformationen öffentlich veröffentlicht hat, kann der Reporter die Sicherheitslücke gerne öffentlich diskutieren.

Die Befolgung der CVD ermöglicht es uns, unsere Kunden zu schützen und gleichzeitig öffentliche Offenlegungen zu koordinieren und den Meldenden angemessen für seine Erkenntnisse zu würdigen. Wenn eine gemeldete Schwachstelle ein Produkt eines Anbieters betrifft, benachrichtigt das PSIRT den Anbieter direkt, stimmt sich mit dem Melder ab oder beauftragt ein Koordinierungszentrum eines Drittanbieters.

Weitere Informationen finden Sie unter https://www.honeywell.com/us/en/product-security

TOP COMMERCIAL SECURITY ANGEBOTE

PRO-WATCH® ECOSYSTEM

INTEGRIERTE SICHERHEITSPLATTFORM

- Höchste Sicherheit dank kryptografischem Coprozessor
- TLS 1.2-Verschlüsselung
- Punkt-zu-Punkt-Verschlüsselung mit OSDP v2
- Doppelte Authentifizierung und Biometrie
- Audit- und Compliance-Berichte
- Zugriffskontrolle im transparenten Modus
- Rückverfolgbarkeit von IT-Assets

MB-SECURE ECOSYSTEM

MB-SECURE PRO, ACS PRO, WINMAG
INTEGRIERTE EINBRUCH- UND ZUGANGSKONTROLLE

- Höchste Sicherheit dank kryptografischem Coprozessor
- AES 128-Bit-Verschlüsselung
- Verschlüsselte Ethernet-Verbindung
- TLS 1.2-Verschlüsselung
- IT-Raumsicherheit mit doppelter Authentifizierung

MAXPRO® CLOUD ECOSYSTEM

INKLUSIVE MAXPRO® ACCESS UND MAXPRO® INTRUSION
INTEGRIERTE VIDEO-, EINBRUCH- UND ZUGANGSKONTROLLE

- Von Azure verwaltete Software as a Service (SaaS)
- Alle Daten zwischen Host und Server mit TLS1.2 AES256-Bit verschlüsselt
- 2-Faktor-Authentifizierung
- Punkt-zu-Punkt-Verschlüsselung mit OSDP v2
- Audit- und Compliance-Berichte
- Zweifach-Authentifizierung für Daten- und Technikräume

VIDEOÜBERWACHUNG

IP-KAMERAS DER SERIE 35, 60 UND 70
35-SERIE UND MAXPRO NVRS

- Höchste Sicherheit dank kryptografischem Coprozessor
- Integrierte FIPS/TPM-zertifizierte Verschlüsselungs-Chipsätze
- Sämtliche verschlüsselte Kommunikation (HTTPS) mit Web- und Mobil-Clients
- Punkt-zu-Punkt-Verschlüsselung des Videostreams zum Perimeterschutz

Für mehr Informationen
www.security.honeywell.de
info.security.de@honeywell.com

Honeywell Commercial Security
Novar GmbH
Forumstraße 30
41469 Neuss
Deutschland
Tel. +49 7431/801-0
Honeywell.com

HCS-FY-NIS2-A4-DE-4jul2024

Honeywell
COMMERCIAL SECURITY