KYBERNETICKÁ BEZPEČNOST V SOULADU S NIS2

BEZPEČNÝ ŽIVOTNÍ CYKLUS VÝVOJE (SDLC)

Společnost Honeywell vyvinula robustní systém pro zvažování bezpečnosti na počátku koncepce produktu a během vývoje, jakož i pro reakci na potenciální zranitelnosti stávajících produktů. Tento systém, iniciativa společnosti Honeywell - bezpečný životní cyklus vývoje software (Secure Software Development Life Cycle - SSDLC), se za posledních několik let vyvinul a stal se ještě robustnějším.

Společnost Honeywell bere bezpečnost produktů vážně. Naše produkty procházejí robustním a komplexním režimem penetračního testování. V některých případech se provádí další nezávislé bezpečnostní testování. Kritéria pro toto dodatečné testování a také to, které produkty nebo nabídky jsou k tomu vybrány, jsou přísně chráněné informace.

Máme robustní a komplexní bezpečný životní cyklus vývoje (Secure Development Life Cycle - SDLC) založený na osvědčených postupech a průmyslových standardech, který zahrnuje následující:

- Posouzení bezpečnostních rizik na základě prostředí ohrožení, kterému konkrétní produkt nebo nabídka čelí, a také technických funkcí a potřeb zákazníků
- Bezpečnostní požadavky a bezpečnostní kontroly založené na průmyslových standardech a směrnicích, jako jsou BSIMM, ISA/IEC 99/62443, ISO 27001, PCI DSS, GDPR, OWASP, příslušné místní zákony a předpisy a další v závislosti na produktu nebo nabídce a bezpečnostním riziku posouzení
- Posouzení dopadu na soukromí (Privacy Impact Assessment)
- Modelování hrozeb (Threat Modeling)
- Standardy a postupy Secure by Design, Privacy by Design a Secure Coding
- Statické testování zabezpečení aplikací (SAST, také známé jako skenování zdrojového kódu) k vynucení postupů bezpečného návrhu a kódování. Skenujeme 10 největších zranitelností podle OWASP (OWASP Top 10) a 25 největších zranitelností podle SANS (SANS Top 25) a také jazyková měřítka kvality. Současné nástroje SAST zahrnují SonarQube a Coverity v závislosti na produktových a jazykových potřebách
- Binární skenování k identifikaci využití open source a potenciálních zranitelností
- Formální politika řízení rizik, která vyžaduje konkrétní časové plány pro zmírnění na základě závažnosti
- Kontrola a schválení kybernetické bezpečnosti nejvyšším vedením před odesláním produktu
- Podpora životního cyklu a upozornění zákazníků na aktualizace zabezpečení

Auditorský tým společnosti Honeywell provádí kontroly, aby zajistil, že jsou dokončeny dodávky zabezpečení požadované v rámci procesů bezpečného životního cyklu vývoje (SDLC) společnosti Honeywell.

Honeywell dokončuje školicí programy pro své zaměstnance o bezpečnostním procesu společnosti a o konkrétních problémech a řešeních v oblasti kybernetické bezpečnosti.

Všichni softwaroví inženýři v Honeywell absolvují formální školení o procesu bezpečného životního cyklu vývoje (SDLC) a obecných tématech kybernetické bezpečnosti/bezpečnosti produktů.

SMĚRNICE O BEZPEČNOSTI SÍTĚ A INFORMACÍ 2 (NIS2)

Směrnice Evropského Parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2)

Požadavky EU na kybernetickou bezpečnost zavedené v roce 2016 směrnicí NIS byly aktualizovány a posíleny směrnicí NIS2, která vstoupila v platnost v roce 2023. Ve světle rostoucí digitalizace s rostoucími kybernetickými útoky a vyvíjejícím se celkovým prostředím kybernetických hrozeb zavedla EU přísnější dohled opatření s kapacitami reakce na incidenty a přísnějšími požadavky na vymáhání jejich rozšířením na nová odvětví a subjekty.

Do 17. října 2024 musí všechny členské země EU přijmout a zveřejnit opatření nezbytná pro dosažení souladu se směrnicí NIS2 a tato opatření začnou uplatňovat od 18. října 2024.

Honeywell

ZÁSADY HLÁŠENÍ O KYBERNETICKÉ BEZPEČNOSTI HONEYWELL

Cílem našeho týmu PSIRT (Product Security Incident Response Team) je minimalizovat riziko zákazníků spojené s bezpečnostními zranitelnostmi poskytováním včasných informací, pokynů a nápravy zranitelných míst v našich produktech, včetně softwaru a aplikací, hardwaru a zařízení, služeb a řešení. Tento tým řídí příjem, vyšetřování, interní koordinaci, nápravu a zveřejňování informací o bezpečnostních slabinách souvisejících s produkty Honeywell.

PSIRT koordinuje reakci a odhalení všech externě identifikovaných zranitelností produktu.

HLÁŠENÍ POTENCIÁLNÍHO ZABEZPEČENÍ ZRANITELNOST

Vítáme zprávy od nezávislých výzkumníků, průmyslových organizací, prodejců a zákazníků zabývajících se bezpečností produktů. Chcete-li zjistit více informací o tom, jak nahlásit potenciální zranitelnost, navštivte webovou stránku Hlášení zranitelnosti na adrese https://www.honeywell.com/us/en/product-security#vulnerability-reporting

KOORDINOVANÉ ZVEŘEJNĚNÍ ZRANITELNOSTI (CVD)

Snažíme se dodržovat Coordinated Vulnerability Disclosure (CVD). Tento proces umožňuje nezávislým reportérům, kteří objeví zranitelnost, kontaktovat přímo Honeywell a dává nám příležitost prošetřit a napravit zranitelnost předtím, než reportér zveřejní informace.

PSIRT bude po celou dobu koordinovat s oznamovatelem průběh vyšetřování zranitelnosti a poskytne mu aktuální informace o pokroku podle potřeby. S jejich souhlasem může PSIRT rozpoznat oznamovatele na základě našich potvrzení o nalezení platné zranitelnosti produktu a soukromého nahlášení problému. Poté, co společnost Honeywell zveřejní informace o aktualizaci, může oznamovatel o zranitelnosti veřejně diskutovat.

Dodržování CVD nám umožňuje chránit naše zákazníky a zároveň koordinovat zveřejnění a patřičně potvrdit oznamovateli jejich zjištění. Pokud se nahlášená chyba zabezpečení týká produktu dodavatele, PSIRT uvědomí přímo prodejce, koordinuje se s oznamovatelem nebo zapojí koordinační centrum třetí strany.

Další informace najdete na https://www.honeywell.com/us/en/product-security

KLÍČOVÉ NABÍDKY KYBERZABEZPEČENÍ OD HONEYWELL

EKOSYSTÉM PRO-WATCH®

INTEGROVANÁ BEZPEČNOSTNÍ PLATFORMA

- Nejvyšší bezpečnost díky kryptografickému koprocesoru
- Šifrování TLS 1.2
- Šifrování point to point s OSDP V2
- Duální ověřování a biometrie
- Audit a reporting shody
- Řízení přístupu v transparentním režimu
- Sledovatelnost IT majetku

EKOSYSTÉM MB-SECURE*

MB-SECURE PRO, ACS PRO, WINMAG INTEGROVANÁ KONTROLA VNIKNUTÍ A PŘÍSTUPU

- Nejvyšší bezpečnost díky kryptografickému koprocesoru
- 128bitové šifrování AES
- Šifrované ethernetové připojení
- Šifrování TLS 1.2
- Zabezpečení IT místnosti s duální autentizací

EKOSYSTÉM MAXPRO® CLOUD

VČETNĚ MAXPRO® ACCESS & MAXPRO® INTRUSION INTEGROVANÉ VIDEO, KONTROLA VNIKNUTÍ A PŘÍSTUPU

- Software jako služba (SaaS) spravovaný Azure
- Všechna data mezi hostitelem a serverem šifrována pomocí TLS1.2 AES256 bit
- 2-faktorové ověřování
- Šifrování point to point s OSDP V2
- Audit a reporting shody
- Dvojité ověření pro datové a technické místnosti

VIDEO DOHLED

IP KAMERY ŘADY 35, 60 A 70 35 SÉRIE A MAXPRO® NVRS

- Nejvyšší bezpečnost díky kryptografickému koprocesoru
- Vestavěné šifrovací čipové sady s certifikací FIPS/TPM
- Veškerá šifrovaná komunikace (HTTPS) s webovými a mobilními klienty
- Point to point šifrování video streamu pro ochranu perimetru

**V současné době k dispozici v DACH a východní Evropě a brzy v dalších evropských zemích.*

Další informace
hwll.co/securityuk
https://buildings.honeywell.com

Honeywell Commercial Security
Building 5, Carlton Park
King Edward Avenue,
Narborough,
Leicester LE19 0LF
Tel: +44(0)1163500714
Honeywell.com

HCS-FY-NIS2-A4-CZ-28aug2024
© 2024 Honeywell International Inc.

Honeywell
COMMERCIAL SECURITY