CYBERBEZPIECZEŃSTWO ZGODNE Z NIS2

PROCES BEZPIECZNEGO CYKLU ŻYCIA I ROZWOJU (SDLC)

Firma Honeywell opracowała solidny system uwzględniania bezpieczeństwa na początku koncepcji produktu i podczas jego opracowywania, a także reagowania na potencjalne luki w istniejących produktach. System ten - Secure Software Development Lifecycle (SSDLC) będący inicjatywą Honeywell, który można tłumaczyć jako bezpieczny cykl życia i rozwoju oprogramowania, ewoluował i stał się jeszcze bardziej niezawodny w ciągu ostatnich kilku lat.

Honeywell poważnie traktuje bezpieczeństwo produktów. Nasze produkty przechodzą przez solidny i kompleksowy program testów penetracyjnych. W niektórych przypadkach przeprowadzane są dodatkowe niezależne testy bezpieczeństwa. Kryteria tych testów oraz to, które produkty lub oferty są do nich wybierane, stanowią ściśle zastrzeżone informacje.

Nasz solidny i kompleksowy proces bezpiecznego cyklu życia i rozwoju (SDLC - Secure Development Life Cycle) oparty na najlepszych praktykach i standardach branżowych obejmuje następujące elementy:

- Ocena ryzyka bezpieczeństwa oparta na środowisku zagrożeń, na jakie narażony jest dany produkt lub oferta, a także na cechach technicznych i potrzebach klienta
- Audyty i kontrole wymogów bezpieczeństwa opartych na standardach i wytycznych branżowych, takich jak BSIMM, ISA/IEC 99/62443, ISO 27001, PCI DSS, RODO, OWASP, obowiązujących lokalnych przepisach i regulacjach oraz innych, w zależności od produktu lub oferty oraz oceny ryzyka bezpieczeństwa
- Ocena wpływu na prywatność (PIA)
- Modelowanie zagrożeń (Threat Modeling)
- Standardy i praktyki Secure by Design Privacy by Design i Secure Coding
- Statyczne testy bezpieczeństwa aplikacji (SAST) znane również jako skanowanie kodu źródłowego, w celu egzekwowania bezpiecznych praktyk projektowania i kodowania. Skanujemy pod kątem luk w zabezpieczeniach zawartych w raporcie podatności aplikacji webowych OWASP Top 10 oraz w raporcie 25 najgroźniejszych błędów oprogramowania SANS Top 25, a także pod kątem wskaźników jakości specyficznych dla danego języka. Obecne narzędzia SAST obejmują statyczną analizę kodu (SonarQube) i statyczną analizę skanowania pokrycia kodu (Coverity) w zależności od potrzeb produktowych i językowych
- Skanowanie binarne w celu identyfikacji wykorzystania oprogramowania typu “open source” i potencjalnych luk w zabezpieczeniach
- Formalna polityka zarządzania ryzykiem, wymagająca konkretnych harmonogramów działań łagodzących w zależności od stopnia ryzyka
- Przegląd i zatwierdzanie cyberbezpieczeństwa produktów przed dostawą przez kierownictwo wyższego szczebla
- Wsparcie cyklu życia produktów i powiadamianie klientów o aktualizacjach zabezpieczeń.

Zespół audytowy firmy Honeywell przeprowadza kontrole w celu zapewnienia, że wymagane w ramach procesów bezpiecznego cyklu życia i rozwoju (SDLC) zadania dotyczące bezpieczeństwa zostały zrealizowane.

Firma Honeywell realizuje programy szkoleniowe dla swoich pracowników na temat procesu bezpieczeństwa firmy oraz konkretnych problemów i rozwiązań z zakresu cyberbezpieczeństwa. Wszyscy inżynierowie oprogramowania w firmie Honeywell przechodzą formalne szkolenie w zakresie procesu bezpiecznego cyklu życia i rozwoju (SDLC) oraz ogólnych zagadnień związanych z cyberbezpieczeństwem i bezpieczeństwem produktów.

DYREKTYWA NIS2 (NETWORK AND INFORMATION SECURITY DIRECTIVE 2)

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS2)

Wymogi UE w zakresie cyberbezpieczeństwa wprowadzone w 2016 r. na mocy dyrektywy NIS zostały zaktualizowane i wzmocnione dyrektywą NIS2, która weszła w życie w 2023 r. W świetle zwiększonej cyfryzacji wraz z rosnącymi atakami cybernetycznymi i ewoluującym ogólnym krajobrazem zagrożeń cyberbezpieczeństwa, UE wprowadziła bardziej rygorystyczne środki nadzoru obejmujące zasady reagowania na incydenty i surowsze wymogi egzekwowania prawa rozszerzając je na nowe sektory i podmioty.

Do dnia 17 października 2024 r. wszystkie państwa członkowskie UE muszą przyjąć i opublikować środki niezbędne do zapewnienia zgodności z dyrektywą NIS2 oraz zacząć je stosować od dnia 18 października 2024 r.

Honeywell

POLITYKA RAPORTOWANIA HONEYWELL W ZAKRESIE CYBERBEZPIECZEŃSTWA

Celem naszego Zespołu Reagowania na Incydenty Bezpieczeństwa Produktu (PSIRT - Product Security Incident Response Team) jest minimalizowanie ryzyka klientów związanego z lukami w zabezpieczeniach poprzez dostarczanie aktualnych informacji, wskazówek i naprawę luk w zabezpieczeniach naszych produktów, w tym oprogramowania i aplikacji, sprzętu i urządzeń, usług i rozwiązań. Zespół ten zarządza przyjmowaniem, dochodzeniem, wewnętrzną koordynacją, naprawą i ujawnianiem informacji o lukach w zabezpieczeniach produktów Honeywell. Zespół PSIRT koordynuje reakcję i ujawnianie wszystkich zidentyfikowanych zewnętrznie luk w zabezpieczeniach produktów.

ZGŁASZANIE POTENCJALNEGO ZAGROŻENIA W BEZPIECZEŃSTWIE

Przyjmujemy raporty od niezależnych badaczy, organizacji branżowych, dostawców i klientów zainteresowanych bezpieczeństwem produktów. Aby uzyskać więcej informacji na temat zgłaszania potencjalnej luki, odwiedź stronę internetową dotyczącą zgłaszania luk w zabezpieczeniach pod adresem https://www.honeywell.com/us/en/product-security#vulnerability-reporting

SKOORDYNOWANY PROCES UJAWNIANIA POTENCJALNEGO ZAGROŻENIA (CVD)

W firmie Honeywell przestrzegamy skoordynowanego procesu ujawniania potencjalnych zagrożeń w zabezpieczeniach (CVD - Coordinated Vulnerability Disclosure). Umożliwia on niezależnym reporterom, którzy odkryją lukę w zabezpieczeniach, bezpośredni kontakt z Honeywell, co daje nam możliwość zbadania i naprawienia luki, zanim zgłaszający ujawni informacje publicznie.

Zespół PSIRT koordynuje działania zgłaszającego przez cały czas badania luki w zabezpieczeniach i, w stosownych przypadkach, dostarcza mu aktualne informacje na temat postępów. PSIRT może docenić zgłaszającego za znalezienie prawidłowej luki w produkcie oraz prywatne zgłoszenie problemu i za jego zgodą umieścić jego dane w zakładce „Podziękowania" na stronie internetowej Honeywell dotyczącej bezpieczeństwa produktów.

Po publicznym opublikowaniu przez firmę Honeywell informacji o aktualizacji lub środkach zaradczych osoba zgłaszająca może publicznie omówić lukę. Przestrzeganie procesu CVD pozwala chronić naszych klientów, a jednocześnie koordynować publiczne zgłoszenia i odpowiednio docenić zgłaszających za wykryte zagrożenia. Jeżeli zgłoszona luka dotyczy produktu dostawcy, PSIRT powiadamia bezpośrednio dostawcę, koordynuje działania ze zgłaszającym lub angażuje zewnętrzne centrum koordynacyjne.

Więcej informacji można znaleźć na stronie https://www.honeywell.com/us/en/product-security

PORTFOLIO O NAJWYŻSZYCH STANDARDACH CYBERBEZPIECZEŃSTWA

EKOSYSTEM PRO-WATCH*

KOMPLEKSOWA PLATFORMA INTEGRUJĄCA

- Najwyższy poziom bezpieczeństwa dzięki koprocesorowi kryptograficznemu
- Szyfrowanie TLS 1.2
- Szyfrowanie Point-to-Point (P2PE) za pomocą OSDP v2
- Uwierzytelnienie dwuskładnikowe (2FA) i biometria
- Audyt i raportowanie zgodności
- Czytniki kontroli dostępu w trybie transparentnym
- Kontrola zasobów IT

EKOSYSTEM MB-SECURE*

MB-SECURE PRO, ACS PRO, WINMAG INTEGRACJA SSWIN I SKD

- Najwyższy poziom bezpieczeństwa dzięki koprocesorowi kryptograficznemu
- Szyfrowanie AES 128-bitowe
- Szyfrowane połączenie Ethernet
- Szyfrowanie TLS 1.2
- Zabezpieczenie pomieszczeń IT/serwerowni z uwierzytelnieniem dwuskładnikowym (2FA)

EKOSYSTEM MAXPRO® CLOUD

W TYM MAXPRO® ACCESS & MAXPRO® INTRUSION INTEGRACJA CCTV, SSWIN I SKD

- Oprogramowanie jako usługa (SaaS) zarządzane przez platformę Azure
- Wszystkie dane szyfrowane TLS1.2 AES 256-bit pomiędzy hostem a serwerem
- Uwierzytelnienie dwuskładnikowe (2FA)
- Szyfrowanie Point-to-Point (P2PE) za pomocą OSDP v2
- Audyt i raportowanie zgodności
- Uwierzytelnienie dwuskładnikowe (2FA) dla archiwów danych czy pomieszczeń technicznych

TELEWIZJA DOZOROWA

KAMERY IP SERII 35, 60 I 70 REJESTRATORY SERII 35 I MAXPRO®

- Najwyższy poziom bezpieczeństwa dzięki koprocesorowi kryptograficznemu
- Wbudowane certyfikowane chipsety szyfrujące FIPS/TPM
- Pełna szyfrowana komunikacja (HTTPS) z Klientem Sieciowym i Mobilnym
- Szyfrowanie Point-to-Point (P2PE) strumienia wideo w ochronie obwodowej

For more information
hwll.co/securityuk
https://buildings.honeywell.com

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

HCS-FY-NIS2-A4-PL-24 June2024

Honeywell
COMMERCIAL SECURITY