CONFORME ALLA NIS2 CYBER SECURITY

PROCESSO “SECURE DEVELOPMENT LIFE CYCLE”

Honeywell ha sviluppato un sistema robusto per considerare la sicurezza fin dall’inizio della concezione del prodotto e durante lo sviluppo, nonché per rispondere a potenziali vulnerabilità nei prodotti esistenti. Questo sistema, l’iniziativa “Secure Software Development Lifecycle” (SSDLC) di Honeywell, si è evoluto ed è diventato ancora più robusto negli ultimi anni.

Honeywell prende molto sul serio la sicurezza dei prodotti. I nostri prodotti sono sottoposti a un rigoroso e completo regime di test di penetrazione. In alcuni casi, vengono condotti ulteriori test di sicurezza indipendenti. I criteri per questi test aggiuntivi, così come i prodotti o le offerte selezionate per questi, sono informazioni proprietarie strettamente riservate.

Il processo Secure Development Life Cycle (SDLC) è basato sulle migliori pratiche e standard industriali che includono:

- Valutazione del rischio di sicurezza basata sulle minacce affrontate da un particolare prodotto o offerta, nonché sulle caratteristiche tecniche e sulle esigenze dei clienti.
- Requisiti di sicurezza e controlli di sicurezza basati su standard e linee guida industriali come BSIMM, ISA/IEC 99/62443, ISO 27001, PCI DSS, GDPR, OWASP, leggi e regolamenti locali applicabili, e altri a seconda del prodotto o dell’offerta e della Valutazione del rischio di sicurezza.
- Valutazioni dell’impatto sulla privacy.
- Modelli di minaccia.
- Standard e pratiche di Secure by Design, Privacy by Design e codifica sicura.
- Test di sicurezza delle applicazioni statiche (SAST, noto anche come scansione del codice sorgente) per far rispettare pratiche di progettazione e codifica sicure. Scansioniamo per le vulnerabilità OWASP Top 10 e SANS Top 25, nonché per misure di qualità specifiche del linguaggio. Gli attuali strumenti SAST includono SonarQube e Coverity, a seconda delle esigenze del prodotto e del linguaggio.
- Scansione binaria per identificare l’uso di open source e le potenziali vulnerabilità.
- Una politica formale di gestione del rischio che richiede tempistiche specifiche di mitigazione basate sulla gravità.
- Revisione e approvazione della cybersecurity da parte della leadership senior prima della spedizione del prodotto.
- Supporto del ciclo di vita e notifica ai clienti per aggiornamenti di sicurezza.

Un team di audit di Honeywell esegue controlli per garantire che i requisiti di sicurezza richiesti dai processi del “Secure Development Life Cycle” di Honeywell siano completati.

Honeywell completa programmi di formazione per i suoi dipendenti sul processo di sicurezza dell’azienda e su preoccupazioni e soluzioni specifiche di cybersecurity.

Tutti gli ingegneri software di Honeywell ricevono una formazione strutturata sul processo del Secure Development Life Cycle e sugli argomenti generali di sicurezza informatica/prodotto.

DIRETTIVA 2 SULLA SICUREZZA DELLE RETI E DELL’INFORMAZIONE (NIS2)

Direttiva (UE) 2022/2555 del Parlamento Europeo e del Consiglio del 14 dicembre 2022 sulle misure per un elevato livello comune di cibersicurezza in tutta l’Unione, che modifica il Regolamento (UE) n. 910/2014 e la Direttiva (UE) 2018/1972, e abroga la Direttiva (UE) 2016/1148 (Direttiva NIS).

I requisiti di cibersicurezza dell’UE introdotti nel 2016 dalla Direttiva NIS sono stati aggiornati e rafforzati dalla Direttiva NIS2, entrata in vigore nel 2023.

Alla luce della crescente digitalizzazione, degli attacchi informatici in aumento e di un panorama complessivo delle minacce alla cibersicurezza in evoluzione, l’UE ha introdotto misure di supervisione più rigorose con capacità di risposta agli incidenti e requisiti di applicazione più severi, estendendoli a nuovi settori ed enti.

Entro il 17 ottobre 2024, tutti i paesi membri dell’UE devono adottare e pubblicare le misure necessarie per conformarsi alla Direttiva NIS2 e devono applicare tali misure a partire dal 18 ottobre 2024.

Honeywell

POLITICA DI SEGNALAZIONE DELLA CYBERSICUREZZA DI HONEYWELL

L'obiettivo del nostro "Product Security Incident Response Team" (PSIRT) è minimizzare il rischio dei clienti associato alle vulnerabilità di sicurezza fornendo informazioni tempestive, linee guida e rimedi per le vulnerabilità nei nostri prodotti, inclusi software e applicazioni, hardware e dispositivi, servizi e soluzioni. Questo team gestisce la ricezione, l'indagine, il coordinamento interno, la risoluzione e la divulgazione delle informazioni sulle vulnerabilità di sicurezza relative ai prodotti Honeywell.

Il PSIRT coordina la risposta e la divulgazione di tutte le vulnerabilità dei prodotti identificate esternamente.

SEGNALAZIONE DI UNA POTENZIALE VULNERABILITÀ DI SICUREZZA

Accogliamo con favore le segnalazioni da parte di ricercatori indipendenti, organizzazioni industriali, fornitori e clienti preoccupati per la sicurezza dei prodotti. Per ulteriori informazioni su come segnalare una potenziale vulnerabilità, visitare la pagina web Segnalazione delle Vulnerabilità all'indirizzo https://www.honeywell.com/us/en/product-security#vulnerabilityreporting.

DIVULGAZIONE COORDINATA DELLE VULNERABILITÀ (CVD)

Ci impegniamo a seguire il nostro processo di Divulgazione Coordinata delle Vulnerabilità (CVD). Questo processo consente ai segnalatori indipendenti che scoprono una vulnerabilità di contattare direttamente Honeywell e ci permette di investigare e risolvere la vulnerabilità prima che il segnalatore divulghi l'informazione al pubblico.

Il PSIRT si coordinerà con il segnalatore durante l'indagine sulla vulnerabilità e fornirà aggiornamenti sui progressi, se appropriato. Con il suo consenso, il PSIRT può riconoscere il segnalatore nei nostri ringraziamenti per aver trovato una vulnerabilità reale nel prodotto e aver segnalato privatamente il problema. Dopo che un aggiornamento o le informazioni di mitigazione sono state rilasciate pubblicamente da Honeywell, il segnalatore sarà libero di a discutere pubblicamente la vulnerabilità.

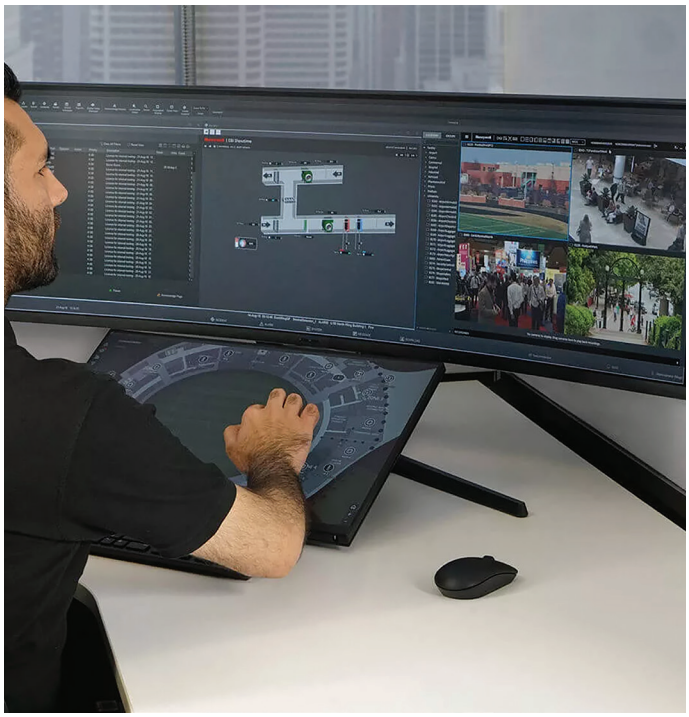
Seguire il processo CVD ci permette di proteggere i nostri clienti e allo stesso tempo coordinare le divulgazioni pubbliche e riconoscere adeguatamente il segnalatore per la sua scoperta. Se una vulnerabilità segnalata riguarda un prodotto di un fornitore, il PSIRT notificherà direttamente il fornitore, coordinerà con il segnalatore o coinvolgerà un centro di coordinamento di terze parti.

Per ulteriori informazioni, si prega di fare riferimento a: https://www.honeywell.com/us/en/product-security.

SOLUZIONI VIDEO, CONTROLLO ACCESSI E ANTINTRUSIONE DI HONEYWELL COMMERCIAL SECURITY

Le diverse gamme di prodotti di Honeywell Security offrono molteplici caratteristiche e funzionalità che possono aiutare le organizzazioni a migliorare la loro cybersicurezza per facilitare la conformità alla direttiva NIS2, come ad esempio:

- Massima sicurezza grazie ai co-processori crittografici
- Chipset di crittografia integrati certificati FIPS/TPM
- Tipi di crittografia: TLS 1.2, AES 128/256 bit, crittografia end to end con OSDP v2, crittografia end to end del flusso video
- Connessione Ethernet crittografata e comunicazioni crittografate (HTTPS) con client web e App mobile
- Autenticazione multifattore e biometria per IT, sale dati e tecniche
- Rapporti di audit e conformità
- Lettori di controllo accessi in modalità trasparente
- Tracciabilità degli asset IT



Per maggiori informazioni
hwll.co/securityit
https://buildings.honeywell.com

Honeywell Commercial Security
Via Achille Grandi 22
20097 San Donato Milanese
Milano
Italia
Tel: +34 902 667 800
Honeywell.com

HBA-SEC-NIS2-FLY-IT-V2-July24-C

Honeywell
COMMERCIAL SECURITY