Panasonic
INDUSTRY

PANNELLI OPERATORE

Guida alla sicurezza

Serie HM

Versione 1.0

2024.07 | https://industry.panasonic.eu/

Copyright e responsabilità

Informazioni sul copyright e sulla responsabilità relative a questa documentazione.

Caroline-Herschel-Strasse 100, 85521 Ottobrunn, Germania

Ultima modifica: 2024-07-23

Panasonic Industry Europe segue una politica di continuo miglioramento del design e delle prestazioni dei suoi prodotti. Pertanto ci riserviamo il diritto di modificare la documentazione/il prodotto senza preavviso. In nessun caso Panasonic Industry Europe potrà essere ritenuta responsabile di eventuali danni diretti, speciali, accidentali o consequenziali derivanti da difetti del prodotto o della relativa documentazione, anche se a conoscenza della possibilità del verificarsi di tali danni.

Per il supporto tecnico contattare Panasonic hotline.

Contenuto

1 Informazioni su questo documento

I rischi interni ed esterni per la cyber security continuano ad aumentare con il progredire della digitalizzazione e la crescente interconnettività dei network.

Il BSI (Ufficio Federale Tedesco per la Sicurezza Informatica), per esempio, ha pubblicato una relazione con le dieci principali minacce e ha definito regole e raccomandazioni per i prodotti impiegati in network nei sistemi di controllo industriale (ICS):

- Infiltrazione di malware tramite supporti rimovibili e hardware esterno
- Infezione malware via Internet e Intranet
- Errore umano e sabotaggio
- Compromissione di componenti extranet e cloud
- Ingegneria sociale e phishing
- Attacchi (D)Dos
- Componenti di controllo collegati a Internet
- Intrusione tramite accesso remoto
- Malfunzionamenti tecnici e forza maggiore
- Compromissione di smartphone nell'ambiente di produzione

Fonte: https://www.bsi.bund.de/ICS

Il presente documento contiene le informazioni sul dispositivo necessarie per la gestione del vostro network e vi aiuterà a proteggere il pannello operatore touch screen serie HM dai rischi per la sicurezza.

2 Criteri di sicurezza per i prodotti Panasonic

I prodotti e servizi Panasonic sono continuamente migliorati. Lo sviluppo dei nostri prodotti segue rigorosamente le regole di sicurezza ed esegue test approfonditi prima della spedizione. La politica di sicurezza di Panasonic si basa sulle linee guida internazionali stabilite da IEC 62443 e ISO/IEC 27001.

Il Panasonic Product Security Incident Response Team (Panasonic PSIRT) è il centro di coordinamento in materia di vulnerabilità associata ai prodotti Panasonic.

3 Configurazione di default del pannello operatore serie HM

Le capacità di network integrate nel pannello operatore touch screen serie HM costituiscono un potenziale di rischio per la sicurezza. Per eliminare o minimizzare tale rischio occorre customizzare le impostazioni di default.

- A partire dalla produzione di maggio 2024 non sarà più possibile impostare una password predefinita e alla prima connessione al dispositivo sarà necessario impostare una password con un minimo di regole predefinite. Le versioni precedenti hanno una password predefinita in fabbrica e si consiglia di cambiarla il prima possibile.
- Le porte Ethernet sono configurate come client DHCP.
- Le porte seguenti sono aperte e in modalità di ascolto per default:

Porta n.°	Protocollo	Funzione
80, 8000, 443	TCP	Utilizzata per la configurazione di browser e pagine web di utenti
53	TCP	Utilizzata per servizio DNS
990-991	UDP	Utilizzata per individuazione di dispositivi tramite broadcast
21 (BSP 1.0 prima del 05/2024)	TCP	Porte dati FTP (modalità FTP passiva: 16384-17407/TCP)
18756-18759	TCP	Porte dati FTP, protette
990 (da BSP 1.3 05/2024)	TCP	Runtime e gestione dei progetti

- Tutte le funzioni e i servizi del pannello operatore touch screen serie HM che potrebbero presentare un rischio di vulnerabilità informatica sono stati disattivati in fabbrica, ad eccezione della funzione script di autorun. I servizi sono elencati in IP/machine_config/#/services.

Servizio	Rischio per la sicurezza
Script di autorun	Applicazioni avviate da un dispositivo di memorizzazione esterno, ad esempio una chiavetta USB
Avahi daemon	Apre la porta 5353 (utilizzata per raccogliere informazioni e trovare funzioni)
Servizio cloud	Ad esempio una configurazione di server OpenVPN utilizzata precedentemente
Server DHCP	Apre le porte 67, 68
Server SNMP	Apre le porte 161, 10161 (utilizzate per raccogliere informazioni)
Server SSH	Apre la porta 22 (login con credenziali di amministratore ed esecuzione di comandi)
Server VNC	Apre la porta 5900 (sito web e controllo dispositivi)

- Il firewall applicato nel pannello operatore touch screen serie HM (IP/machine_config/#/services) è disattivato per default.

- Il pannello operatore touch screen serie HM scrive dati di log e informazioni di utilizzo atipiche in file di log. Questi file sono archiviati nel dispositivo e possono essere scaricati con le credenziali di amministratore.

NOTA

Utilizzate il firewall per chiudere tutte le porte non utilizzate, ma fate attenzione che la porta Ethernet 443 sia aperta e compresa nella configurazione del firewall (per BSP 1.0 è necessario che anche la porta 80 sia aperta). Altrimenti l'accesso alla pagina di impostazione del sistema sarà permanentemente negato.

Argomenti correlati

Impostazione di firewall (pagina 11)

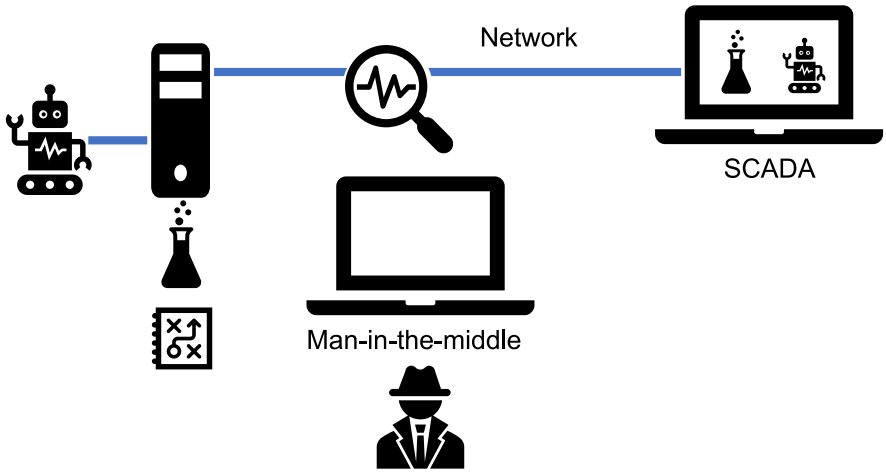
4 Potenziali scenari di minaccia

Per aumentare la vostra consapevolezza degli scenari di minaccia e per una miglior comprensione, vi diamo alcuni esempi tipici di potenziali cyber minacce.

- Cattura dei dati

  Per leggere il traffico di dati nel network, compresi nomi utente, password e altri dati sensibili, come ricette o dati di processo, sono disponibili numerosi strumenti.

  Soprattutto se il vostro traffico nella rete non è crittografato, è un facile bersaglio per spie alla ricerca di informazioni leggibili.

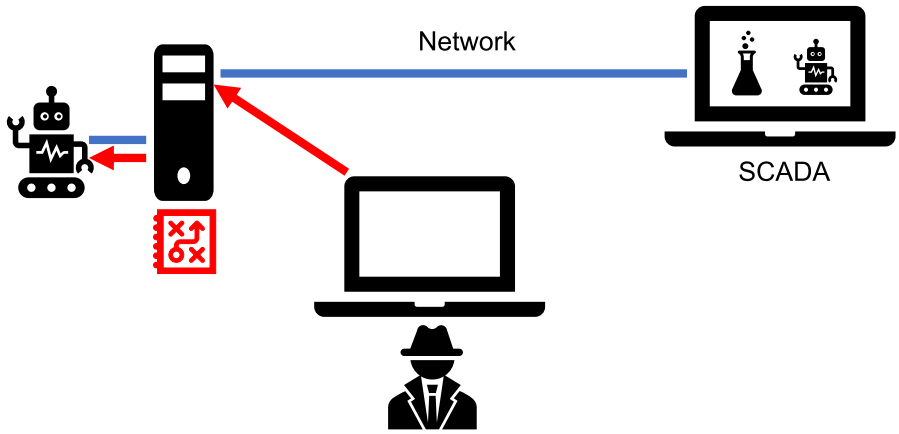


  Contromisure:

  Non utilizzate protocolli FTP o Telnet al di fuori di un network incapsulato per trasmettere dati sensibili. Questi protocolli rappresentano un alto rischio per la sicurezza perché i nomi utente e le password sono trasmessi in testi normali.

- Ottenere l'accesso ai sistemi di controllo

  Se credenziali o il protocollo utilizzato sono noti, eventualmente possono essere causati guasti o danni alle macchine e i dispositivi possono essere dirottati in botnet o essere manipolati per attaccare altri dispositivi.

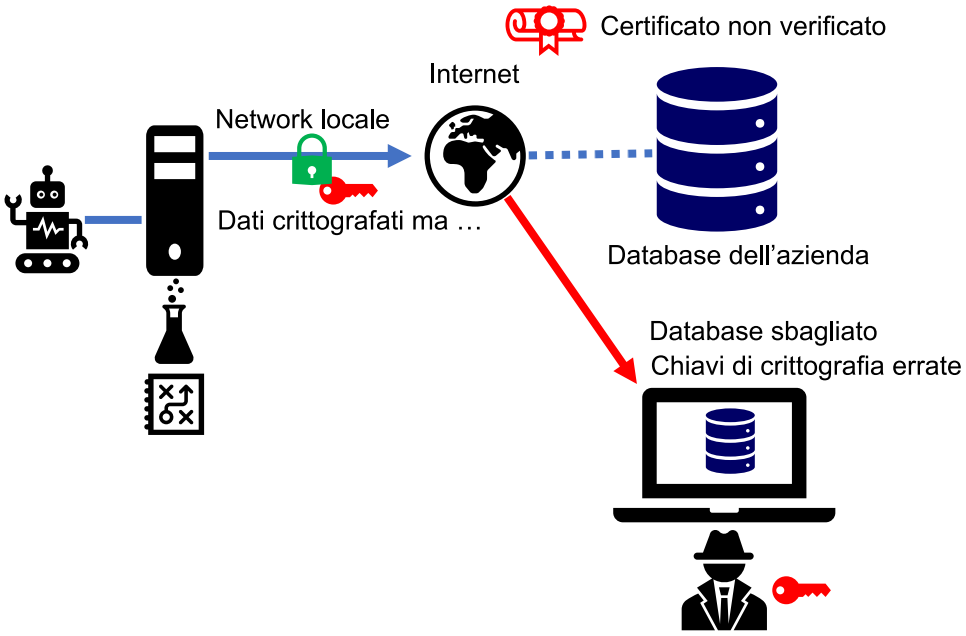


  Contromisure:

  Assicurarsi che computer di terzi non possano avere l'accesso o assumere il controllo.

- Furto di identità

  Le connessioni a pagine web che non sono verificate da un'autorità di certificazione possono essere pericolose perché facilitano il furto di identità e il reindirizzamento di comunicazione. Questo consente ad aggressori di raccogliere informazioni sensibili (ad esempio nomi utente, password, dati di processo o ricette) e di causare danni manipolando macchine.



  Contromisure:

  Accertatevi che si faccia utilizzo di certificati per autenticare l'identità del server di destinazione.

5 Misure di sicurezza generali

Le misure protettive sono essenziali per la sicurezza e la protezione del network e del traffico.

Considerando che l'uso di questo prodotto richiede il collegamento a un network, è opportuno richiamare l'attenzione sui rischi per la sicurezza elencati di seguito.

- Perdita o furto di informazioni per mezzo di questo prodotto
- Uso del prodotto per operazioni illecite da parte di malintenzionati
- Interferenza o interruzione del funzionamento del prodotto da parte di malintenzionati
- L'utente è responsabile di prendere le dovute precauzioni, di cui a seguire si riportano alcuni esempi, per proteggersi dai rischi per la sicurezza delle reti.
- Se questo prodotto è connesso a un network che include dei PC, accertarsi che il sistema non possa infettarsi con virus o altro malware (per mezzo di un antivirus aggiornato regolarmente, un programma anti-spyware ecc.).
- Usate questo prodotto in un ambiente dotato di una LAN, una VPN (rete privata virtuale) o una rete di linee affittate.
- Usate questo prodotto in un ambiente in cui possono entrare solo persone con diritti di accesso controllati.
- Usate questo prodotto e altri dispositivi collegati tramite network, come un PC o un tablet, solo se avete preso misure di protezione per garantire la sicurezza.
- Non installare questo prodotto in locali dove il prodotto o i cablaggi possono essere distrutti o danneggiati da malintenzionati.

È opportuno notare che un'impostazione scorretta alla rete LAN esistente può causare un malfunzionamento dei dispositivi connessi alla rete. Consultare il proprio amministratore di rete prima di effettuare la connessione.

Su Internet si trovano informazioni molto utili: MITRE ATT&CK® è una base di conoscenza accurata e un modello di comportamento degli avversari informatici.

6 Best practice per aumentare la protezione del vostro pannello operatore serie HM

Potete minimizzare i rischi per la sicurezza adottando misure preventive ed effettuando le impostazioni di sistema e di applicazioni giuste. Usate la lista di verifica fornita in questa guida per assicurarvi di prendere tutte le misure necessarie per proteggere il pannello operatore touch screen serie HM.

Argomenti correlati

Lista di verifica della configurazione di sicurezza (pagina 14)

6.1 Impostazioni di sistema

Andate a “System Settings” (Impostazioni di sistema, IP/machine_config) per impostare password e firewall, per accedere a file di log e per utilizzare le funzioni di debug SSH.

6.1.1 Password di protezione

Impostate una password forte che contenga lettere maiuscole e minuscole, numeri e caratteri speciali (tranne spazi vuoti).

Utilizzate password per FTP server diverse per le applicazioni di HMWIN Studio e per le impostazioni principali del pannello operatore touch screen serie HM. Quando si accende un terminale per la prima volta, viene chiesto di inserire una nuova password di sicurezza. Questa operazione può essere eseguita direttamente sul display o tramite un browser collegato al dispositivo tramite il suo indirizzo IP (IP/machine_config).

6.1.2 Impostazione di firewall

Utilizzate il firewall (IP/machine_config/#/services) per chiudere tutte le porte non utilizzate.

Se attivate il “Firewall Service” (IP/machine_config/#/services), tutte le funzioni utilizzate sono attivate con le impostazioni e le porte indicate. Disattivate i servizi non utilizzati o negate l'accesso a interfacce dedicate (ETH0, ETH1 e ETH2).

NOTA

Accertatevi che “Web Server – HTTP” e “Web Server – HTTPS” siano attivati e che la porta Ethernet 443 sia aperta (anche la porta 80 per BSP 1.0). Altrimenti l'accesso alla pagina di impostazione del sistema sarà permanentemente negato.

Esempio di impostazioni di firewall:

Nome	Interfaccia source	Porta o range	Protocollo	Richiesto
Web-Server - HTTP (richiesto per la configurazione)	Qualsiasi	80	TCP	✓ (BSP 1.0)
Web-Server - HTTPS (richiesto per la configurazione)	Qualsiasi	443	TCP	✓
Individuazione di dispositivo	Qualsiasi	990–991	UDP	✓
Porta di comando FTP, occorrente per il funzionamento di HMWIN Studio	Qualsiasi	21	TCP	✓ (BSP 1.0)
Modalità FTP passiva, occorrente per il funzionamento di HMWIN Studio	Qualsiasi	18756–18759	TCP	
Server SSH	Qualsiasi	22	TCP	
Server VNC	Qualsiasi	5900	TCP	
Server DHCP	Qualsiasi	67	UDP	
Server SNMP	Qualsiasi	161	UDP	
Porte di connessione PLC	Qualsiasi	9094–9097	TCP	
Operazioni HMWIN Studio	Qualsiasi	990	TCP	

6.1.3 File di log e funzioni di debug SSH

Queste funzioni possono essere utilizzate per rilevare un utilizzo atipico. Possono essere utilizzate solo con credenziali di amministratore.

7 FAQ

1. Posso ottenere patch software e aggiornamenti del firmware?

   I download gratuiti delle versioni più recenti sono disponibili sul sito web Panasonic: Panasonic Download Center o InfoHub

2. C'è qualche backdoor installata sul dispositivo?

   Non c'è nessuna backdoor installata sul dispositivo. Se perdete la password, non c'è modo di ripristinare le impostazioni.

3. Il dispositivo chiama qualche server Panasonic?

   Con le impostazioni del produttore nessun processo chiama automaticamente un server Panasonic.

4. Dove posso segnalare un nuovo rischio di vulnerabilità informatica?

   Contattare il Panasonic Product Security Incident Response Team (Panasonic PSIRT), il centro di coordinamento in materia di vulnerabilità associata ai prodotti Panasonic.

8 Lista di verifica della configurazione di sicurezza

Usate questa lista di verifica per assicurarvi di prendere tutte le misure necessarie per proteggere il pannello operatore touch screen serie HM. Spuntate tutte le voci che avete completato. Alla fine della lista, c'è spazio per voci aggiuntive.

Verificato	Rischio[1]	Area	Pagina di configurazione	Da fare
	Alto	Password (admin, user)	IP/machine_config/#/ authentication	Passaggio a password di amministrazione e utente sicure
	Alto	Servizio: Script di autorun	IP/machine_config/#/services	Disattivare
	Alto	Servizio: Server SSH	IP/machine_config/#/services	Disattivare se non necessario
	Basso	Avahi daemon	IP/machine_config/#/services	Disattivare se non necessario
	Basso	Servizio cloud	IP/machine_config/#/services	Disattivare se non necessario
	Basso	Server DHCP	IP/machine_config/#/services	Disattivare se non necessario
	Basso	Servizio VNC	IP/machine_config/#/services	Disattivare se non necessario
	Basso	Firewall	IP/machine_config/#/services	Attivare e customizzare le impostazioni
	Alto	Password HMWIN (almeno amministratore, utente, log)	HMWIN Studio Project/Configuration/Security	Cambiare password di default per amministratore e utente
	Alto	Configurazione del protocollo	HMWIN Studio Progetto/Configurazione/ Protocolli	Disattivare le funzioni di pass-through e i protocolli server se non necessari. Scegliere varianti crittografate dei protocolli fieldbus utilizzati
	Medio	Funzione HMWIN OPC UA	HMWIN Studio Project/Configuration/Interface	Verificare l'accesso a server
	Medio	Funzione HMWIN MQTT	HMWIN Studio Project/Configuration/Interface	Utilizzare crittografia e certificati
	Medio	Caratteristiche Javascript SMTP e FTP	HMWIN Studio Controllare gli eventi configurati (ad es. e-mail, FTP, telecamera web ...)	Utilizzare crittografia e certificati

Verificato	Rischio[1]	Area	Pagina di configurazione	Da fare

1) Il livello di rischio dipende dalla vostra applicazione.

9 Panasonic hotline

In caso di domande che non trovano risposte all'interno dei manuali o dell'help online, contattare uno dei nostri uffici vendite.

Potete aiutarci ad avere i seguenti dati a portata di mano:

- Numero di serie del vostro prodotto e/o numero versione.
- Numeri versione e service pack di MS-Windows installati nel vostro computer.
- Tipo di hardware in uso.
- Esatta formulazione di qualsiasi messaggio che appare sulla pagina.
- Che cosa è successo e cosa avete fatto quando si è verificato il problema?
- Come avete tentato di risolvere il problema?

Digita il numero della linea assistenza o utilizza il nostro modulo di contatto per inviarci la tua richiesta.

Per richieste al di fuori dell'Europa, visita il nostro sito web globale.

Panasonic Industry Europe GmbH

- Germania e paesi europei non elencati su questa pagina:
  +49 89 45354-2748 (PLC, FP-I4C, pannelli operatore touch)
  +49 89 45354-2737 (sensori)
  +49 89 45354-2750 (servoazionamenti)
- Francia:
  +33 160 135757

Panasonic Industry Austria GmbH

Austria, Bosnia ed Erzegovina, Bulgaria, Croazia, Montenegro, Serbia, Slovenia, Svizzera:

+43 2236 26846

Panasonic Industry Benelux B.V.

Belgio, Danimarca, Lussemburgo, Norvegia, Svezia, Paesi Bassi:

+31 499 372727

Panasonic Industry Italia srl

Italia:

+39 045 6752711, support.piit@eu.panasonic.com

Panasonic Industry Poland sp. z o.o.

Paesi baltici, Repubblica Ceca, Finlandia, Ungheria, Polonia, Romania, Slovacchia:

+48 42 2309633

Panasonic Industry Iberia S.A.

Portogallo, Spagna:

+34 91 3293875

Panasonic Industry UK Ltd.

Regno Unito e Irlanda:

+44 1908 231555

10 Registrazione di modifiche

Guida alla sicurezza Versione 1.0, 2024.07

Prima edizione italiana