LINEE GUIDA

Ultimo aggiornamento: Marzo 2018

Linee guida *ASERCOM* sulla sicurezza informatica per le apparecchiature HVAC/R

Premessa

Molti componenti delle applicazioni HVAC/R, come ad esempio compressori, ventilatori o controllori elettronici, sono dotati di funzioni di connettività, quali ad esempio il Bluetooth, il Wi-Fi o LAN. La presente linea guida intende fornire dei consigli su come collegare in sicurezza tali componenti HVAC/R a smartphone, altri computer oppure alla rete internet. La struttura della presente linea guida segue il ciclo di vita utile di un impianto HVAC/R: inizia dalla progettazione dell'architettura, prosegue con l'installazione del sistema e la manutenzione dello stesso per tutta la sua durata e termina, infine, con dei consigli sulle azioni da intraprendere durante la dismissione dell'impianto.
Il presente documento fornisce quindi consigli pratici ed indirizzati ad aumentare la sicurezza di tali impianti durante la loro vita operativa. Queste misure possono contribuire a rendere meno vulnerabili i controllori elettronici o gli inverter installati, ma non costituiscono un'alternativa ad un sistema di gestione integrato. In particolare, per gli impianti/imprese di maggiori dimensioni si raccomanda di verificare con attenzione la necessità di applicare un sistema di gestione della sicurezza informatica integrato (ISIM). Per una corretta valutazione di tale aspetto, si rimanda alla consultazione delle norme ISO 27001, UL2900 oppure IEC62443:
(vedere:

- https://www.iso.org/isoiec-27001-information-security.html
- https://en.wikipedia.org/wiki/ISO/IEC_27001
- https://en.wikipedia.org/wiki/Cyber_security_standards
  Kobes, P.: Guideline Industrial Security ISO 62443 is easy; Berlin: VDE Verlag; 2017)

Si consiglia, inoltre, di controllare regolarmente e far riferimento ad eventuali norme locali vigenti in materia di sicurezza informatica. La legislazione, in questo ambito, potrebbe cambiare nel tempo.

Imagine:pixabay

Nota generale

Le normative relative alla sicurezza informatica, come la IEC 62443, VDI/VDE 2182 e altre, definiscono tre diversi soggetti e ruoli in un impianto collegato alla rete internet:

a) Il produttore dei dispositivi collegabili, come controllori elettronici, inverter di frequenza o sensori (definito talvolta anche con il termine di "Venditore")
b) Il System integrator, ovvero colui che progetta e installa il sistema sul campo usando i dispositivi collegabili (definito talvolta anche con il termine di "Appaltatore")
c) Il proprietario delle attività che utilizza le apparecchiature HVAC/R collegate

Questi soggetti hanno un compito molto importante: la comunicazione. Devono scambiarsi tra loro informazioni su specifiche, esigenze, casi d'uso, modifiche ed altro. La sicurezza informatica non è un'attività singola che, una volta raggiunta, si conclude per sempre. È importante aggiornare costantemente le informazioni a disposizione (come nel caso di rilasci di nuovi aggiornamenti) per tutto l'intero ciclo di vita utile del sistema. A tal fine è buona norma istituire un ciclo PDCA (Plan-Do-Check-Act: pianifica-opera-controlla-agisci) che venga seguito durante tutta la vita utile del sistema.
Nelle seguenti sezioni vengono riportate alcune importanti raccomandazioni. In aggiunta, e qualora sia necessario applicare misure di protezione del sistema più complesse, è importante eseguire un'analisi dei rischi individuali. I punti indicati nella presente linea guida riguardano principalmente tecnologia e processi, ma oltre a questi fattori è fondamentale concentrarsi sulle persone: tutti e tre gli attori coinvolti (produttore, System integrator e proprietario delle attività) devono, con regolarità, addestrare e sensibilizzare sulla questione della sicurezza informatica tutti i dipendenti coinvolti.

Non tutti i provvedimenti proposti potrebbero adattarsi a tutti gli impianti e le applicazioni sul campo. È quindi importante selezionare quelli più appropriati e utilizzabili.

Architettura / Programmazione

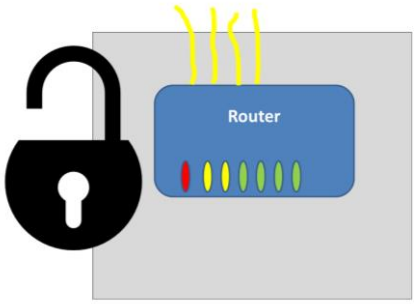
Creare una progettazione secondo il principio della "Defense in-depth"

Rischio: Una singola misura a protezione di un sistema HVAC/R sul campo può facilmente avere punti deboli ed essere vulnerabile.
Soluzione: Anziché affidarsi a una singola contromisura per evitare attacchi informatici, è consigliabile applicare diverse misure di protezione complementari. Se un malintenzionato riesce a superare il primo livello, dovrà affrontarne un secondo e così via.

Posizionare i componenti dell'infrastruttura IT, come ad esempio i router, in un armadietto/stanza chiuso/a a chiave

Rischio: se persone non autorizzate riescono ad accedere fisicamente ai componenti dell'infrastruttura IT, come router, firewall o PLC, possono modificare le impostazioni e ottenere l'accesso all'impianto. Questo aspetto diventa particolarmente importante nel caso di presenza di porte di accesso di tipo USB o similari nei componenti dell'infrastruttura IT.

Soluzione: Posizionare i componenti dell'infrastruttura IT, come router o firewall, in un armadietto o in una stanza dotata di controllo degli accessi (ad esempio chiusa a chiave). Assicurarsi che solo il personale autorizzato possa accedere a questa stanza e che rimanga sempre chiusa in presenza di persone non autorizzate.



Separare le apparecchiature HVAC/R da altre parti della rete (ad esempio dagli uffici) tramite segmentazione della rete (ad esempio tramite firewall)

Rischio: Se l'apparecchiatura HVAC/R si trova nello stesso segmento con altre apparecchiature dell'ufficio o webserver, un eventuale attacco informatico a una parte della rete può facilmente compromettere l'intera infrastruttura.

Soluzione: Suddividere l'impianto in segmenti logici con comunicazione separata (vedere anche https://en.wikipedia.org/wiki/Network_segmentation). Quest'operazione può essere fatta applicando un firewall tra due segmenti.

Fase di installazione / messa in servizio

Modifica delle password predefinite per il login (sia per l'amministratore che per gli utenti)

Rischio: dispositivi quali firewall o router, inverter di frequenza, controllori elettronici e ventole EC dotate di interfaccia web hanno in genere un'interfaccia per login con credenziali di accesso predefinite (nome e password). Di solito tali informazioni sono riportate nel manuale d'uso. Se le credenziali di accesso predefinite non vengono modificate, un malintenzionato può accedere in maniera semplice al dispositivo non appena ne abbia scoperto il relativo indirizzo IP.

Soluzione: le credenziali di default (nome e password) devono essere cambiate durante la fase di installazione.

Dopo l'installazione ricordarsi di cancellare gli account temporanei o di default

Rischio: spesso gli account temporanei (admin o user) vengono impostati dagli appaltatori durante l'installazione e altrettanto spesso utilizzano una password molto semplice per semplificare le operazioni di installazione.

Soluzione: gli account usati durante l'installazione devono essere cancellati non appena terminata l'operazione. In alternativa vanno protetti con una password sicura.

Usare password contenenti lettere, numeri e caratteri speciali con una lunghezza minima di 8 caratteri

Imagine:pixabay

Rischio: con un attacco di tipo password cracking, eseguito mediante dei software automatizzati (ad esempio utilizzando “Medusa”, disponibile nella distro KALI Linux), si possono provare migliaia di password alla ricerca di quella del sistema. Questi strumenti usano elenchi contenenti password oppure generatori casuali (attacchi a dizionario oppure a forza bruta). Le password dei dizionari sono quelle trovate durante precedenti attacchi a provider di servizi Internet oppure ad applicazioni o portali web (ad esempio ebay.com). Contengono inoltre le password usate più frequentemente, come “123456” oppure “password”.

Soluzione: usare password complesse che non siano parole già presenti in un dizionario, aumentare la complessità sostituendo le "i" con gli "1" o le "s" con il "5". Per ridurre il rischio di un’intrusione, la password deve contenere almeno 8 caratteri ed essere casuale. Le password non casuali possono essere anche più lunghe. Si consiglia inoltre di non usare la stessa password in più di un impianto.

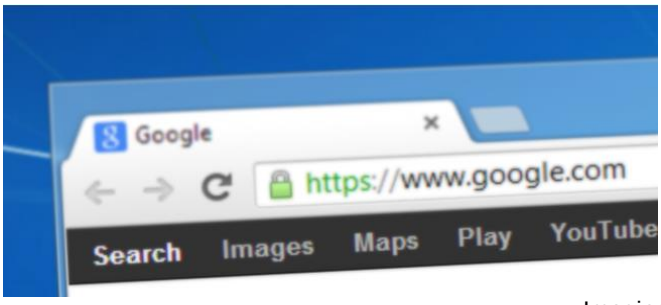
Aumentare la protezione del sistema chiudendo/disattivando le porte, i protocolli e gli indirizzi IP accessibili nei dispositivi collegati.

Rischio: Un indirizzo IP di un dispositivo elettronico / computer può essere paragonato all'indirizzo di una casa, mentre una porta (es. 443) o un protocollo (es. https) all'ingresso di questa casa. Le diverse applicazioni basate sul web, come email, trasferimento di file o siti web, hanno protocolli e porte predefinite. Ogni porta aperta (ovvero accessibile) costituisce un potenziale rischio informatico di intrusione da parte di malintenzionati.

Soluzione: un dispositivo HVAC/R, in genere, accede solo ad un server di manutenzione e utilizza solo funzionalità limitate nel web, perciò gli indirizzi IP accessibili e le porte aperte possono essere notevolmente ridotti. Si consiglia di disabilitare tutti gli indirizzi IP non necessari e di disabilitare tutte le porte non utilizzate. Un sistema di aria condizionata non ha bisogno di vedere i video su youtube.com o consultare wikipedia.org.

Usare trasmissione dati crittografata (https, non http; codifica Bluetooth; VPN…)

Rischio: se i dati vengono trasmessi wireless o via cavo senza crittografia, sussiste sempre il rischio che qualcun altro possa intercettare questa comunicazione, ed ottenere le credenziali di accesso ad un sistema o un dispositivo elettronico.



Imagine:pixabay

Soluzione: per la trasmissione dei dati e la comunicazione devono essere sempre usate la crittografia e l'autenticazione di livello più avanzato. È importante aggiornare continuamente la tecnologia di autenticazione utilizzata, impiegando sempre la migliore disponibile in un dato momento.

Manutenzione durante la vita operativa del sistema

Installare tutti gli aggiornamenti disponibili per firewall, router, smartphone/tablet, PC/portatili ecc. usati nell'impianto HVAC/R.

Rischio: si riscontra regolarmente la scoperta di punti deboli che rendono vulnerabili i dispositivi connessi alla rete internet. Per far fronte a questo, i produttori di software e hardware rilasciano aggiornamenti e patch per i propri prodotti, specie nel caso uno di questi sia stato interessato da un problema di sicurezza. Se un sistema o un componente privo di patch vengono usati in un circuito HVAC/R, questo sistema è vulnerabile ad attacchi informatici.

Soluzione: è necessario installare tutti gli aggiornamenti e tutte le patch disponibili. Molti dispositivi, come firewall e router, possono ricercare automaticamente la presenza di aggiornamenti. In simili casi, il personale addetto alla manutenzione deve attivarsi e installare l'aggiornamento. Oltre ai componenti ed ai software usati in loco al momento dell'installazione di dispositivi HVAC/R è anche necessario che tutti gli "strumenti", come smartphone, portatili o PC che sono momentaneamente collegati al sistema, siano aggiornati.

Disattivare Bluetooth / Wi-Fi se non usati / non necessari

Imagine:pixabay

Rischio: esistono strumenti informatici (hacker tools) in grado di attaccare le connessioni Bluetooth. In un campo libero, una connessione Bluetooth può essere instaurata ad una distanza di 50-100 m. Questo significa che un attacco Bluetooth può partire anche dall'esterno del perimetro sotto controllo (edificio chiuso o proprietà recintata).

Soluzione: nella maggior parte dei casi, una connessione continua via Bluetooth o WiFi non è necessaria. Spesso può restare spenta per gran parte del tempo ed essere attivata solo se qualcuno deve trasmettere dei dati. La disattivazione della connettività wireless, quando non necessaria, permette di aumentare il livello di sicurezza informatica.

Mantenere attive le credenziali di User ed Admin per tutta la vita utile del sistema

Rischio: i dipendenti del proprietario dell'attività o dell'appaltatore possono lasciare l'azienda per cui lavorano durante la vita utile del sistema HVAC/R. Se l'account di questo ex dipendente non viene cancellato, questi potrà ancora accedere all'apparecchiatura collegata a internet.

Soluzione: stabilire una procedura per assicurarsi che gli account di tutti i dipendenti dimissionari vengano disabilitati. Una situazione simile si verifica anche quando il proprietario dell'attività passa dall'appaltatore di servizi A all'appaltatore di servizi B. Se nel dispositivo è disponibile una funzione di password dinamica, si consiglia di usarla.

Dismissione e smantellamento dell’impianto

Resettare tutti i dispositivi, riportandoli alle impostazioni di fabbrica, e cancellare tutte le password e tutti i dati salvati in essi. Password e dati non devono essere rivelati a nessuno dopo la dismissione.

Rischio: se un dispositivo o un sistema ha raggiunto la fine della vita utile, questo viene dismesso. Qualora dei dati siano ancora memorizzati all'interno del dispositivo (ad esempio in un hard-drive all'interno di un PC o una (scheda di) memoria non volatile in un controllore elettronico), questi dati potrebbero diventare accessibili a terzi se il dispositivo non viene dismesso in maniera corretta.

Soluzione: prima di smaltire i dispositivi, assicurarsi che tutti i dati in essi contenuti vengano cancellati e tutte le impostazioni resettate alle impostazioni di fabbrica. Prestare particolare attenzione alle schede di memoria (schede SD), alle memorie USB, alle credenziali di accesso al Cloud ed ai dati memorizzati su smartphone o laptop.

Imagine:pixabay

LINEE GUIDA

Ultimo aggiornamento: Marzo 2018

Indice delle revisioni

Revisione	Modifica	Data
A	Pubblicazione iniziale	22.03.2018