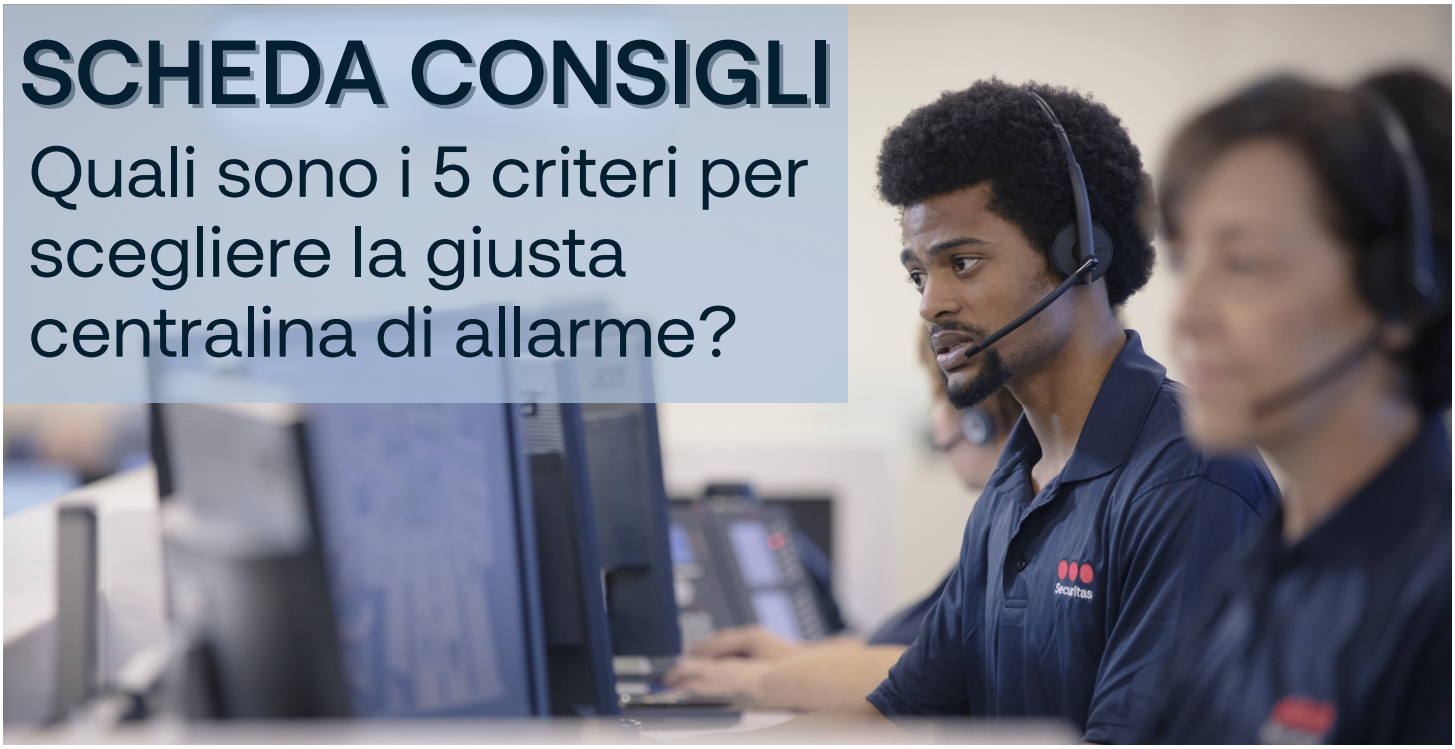
SCHEDA CONSIGLI

Quali sono i 5 criteri per scegliere la giusta centralina di allarme?



Pascal Hulalka,
Solution Director

Questa decisione è uno dei tanti step necessari per predisporre un dispositivo di sicurezza, un'operazione a volte complessa che richiede il giusto supporto.

Per aiutarti a capire che tipo di domande bisogna farsi, il nostro esperto Pascal Hulalka, membro del comitato svizzero per gli standard di trasmissione degli allarmi, elencherà i 5 criteri da considerare quando occorre scegliere una centralina di allarme.

1-PROTEGGERE LA TRASMISSIONE

Dalla fine della rete analogica, in Svizzera gli allarmi vengono trasmessi tramite una rete IP (Internet Protocol). Nonostante sia considerata affidabile, raramente una rete è disponibile al 100%. Ciò significa che, con un'affidabilità statistica del 99,5%, il tuo allarme potrebbe non comunicare per 1,8 giorni all'anno, non avvisandoti qualora si dovesse verificare un'effrazione o un incendio.
Per questo motivo consiglio sempre una trasmissione bidirezionale, anche agli utenti privati, ovvero un IP cablato e un modem 3G o 4G, nel caso in cui la connessione cablata si interrompa. Analogamente, è bene scegliere un fornitore di servizi con una centralina di allarme a ridondanza che la garantisca, oltre che nella trasmissione, sia nella ricezione che nell'elaborazione degli allarmi.

2-CONTROLLARE IL PROPRIO TEMPO DI POLLING

Il polling è una tecnica che consiste nell'interrogare in modo continuo e sequenziale i dispositivi periferici per verificare se hanno dati da trasferire.

Per garantire che la connettività tra il tuo impianto e la centralina di allarme professionale (o il cloud di un produttore) sia operativa, tra i due sistemi vengono inviati piccoli pacchetti di dati (tipo "telegrammi") a intervalli regolari.
Per i privati e le PMI, con un sistema ridondante basta un polling di 24 ore sulla parte IP cablata. Per le strutture più grandi consiglio un tempo di polling di 30 minuti, o addirittura di 3 minuti per banche e gioiellerie.
Inoltre, una volta alla settimana è prassi effettuare un test di routine per verificare che la centralina di allarme funzioni correttamente da un capo all'altro della struttura da proteggere, fino all'operatore della centralina di allarme professionale.

3-PREDILIGERE UN PROTOCOLLO APERTO

Questa questione è spesso oggetto di dibattito, come lo era all'epoca tra i sostenitori e i detrattori dei sistemi operativi Windows e Linux. Ogni sistema presenta vantaggi e svantaggi.
· Un sistema aperto significa maggiore flessibilità quando si tratta di interfacciarsi con l'infrastruttura esistente. Inoltre, un maggior numero di persone può testare e suggerire miglioramenti e modifiche.

Protectas
Rue de Genève 70
1004 Lausanne

+41 21 623 26 00
swiss@protectas.com

www.protectas.com

· Un sistema proprietario o sviluppato da un integratore può essere complicato da installare (sostituire) e quindi più costoso da implementare. Oggi i protocolli aperti SIA DC09 e VdS2465 sono protocolli aperti completi (tipo di eventi, zone, ecc.) e sono quelli che Protectas ha scelto di prediligere. Questo ci permette di allontanarci dai sistemi proprietari e di fornire servizi a prescindere dal sistema di allarme predisposto. Nella fattispecie, la semplice aggiunta di un trasmettitore (di allarme) che utilizza in modo nativo questi protocolli aperti permette di interfacciarsi con il sistema del produttore a un costo ragionevole.

In ogni caso, a prescindere dal tipo di protocollo, la comunicazione criptata è essenziale per ridurre al minimo il rischio di hacking!

4-INTEGRARE ACCERTAMENTI

Avere un sistema cieco è diventato arcaico.
È la prima volta che senti questo specifico termine di sicurezza? Potresti chiederti cosa significa.
L'accertamento è una procedura che prevede l'utilizzo di tutti i mezzi possibili per accertarsi che un'effrazione sia effettivamente in atto. Nella telesorveglianza è un prerequisito essenziale per richiedere l'intervento della polizia.
Qualora le autorità vengano chiamate ingiustificatamente, senza un previo controllo formale, possono scattare sanzioni finanziarie. L'accertamento può essere effettuato in loco o da remoto.
L'accertamento fisico consiste nell'intervenire sul posto dopo che si è attivato un allarme. L'operatore di telesorveglianza che gestisce e riceve i segnali di allarme invia immediatamente una guardia giurata presso la struttura del cliente per stabilire l'origine e la validità dell'allarme. Si tratta di un'operazione di verifica che completa un servizio di telesorveglianza.

Una volta accertato e verificato ciò che ha provocato l'allarme - per esempio un'effrazione - la guardia giurata prenderà le dovute misure precauzionali. Nella maggior parte dei casi chiamerà la polizia, ma può anche effettuare la riparazione d'emergenza di un accesso.
L'accertamento audio o video prevede di collegarsi alla centralina di allarme del cliente per accedere alle registrazioni video/audio, oppure allo stream live delle telecamere/microfoni che monitorano i rilevatori in allarme.
Il tutto avviene quindi telematicamente da remoto, con un enorme risparmio di tempo. L'odierna tecnologia lo rende possibile, mentre il tempo che un operatore deve impiegare per spostarsi non è da sottovalutare.

UTILE DA SAPERE. Il live stream si attiva solo quando viene emesso un allarme. L'operatore di telesorveglianza non può quindi spiarti quando sei a casa.

È quindi fondamentale che i privati o le aziende che dispongono di un sistema di allarme con telesorveglianza integrino il loro dispositivo di sicurezza con un servizio di accertamento fisico, oppure di accertamento video o addirittura audio.

5-GARANTIRE L'AFFIDABILITÀ DEL SISTEMA

I sistemi di allarme vengono valutati in base a diversi criteri, che portano all'assegnazione di una certificazione nota come "normativa sui sistemi di allarmi".
A livello europeo bisogna tenere a mente le 2 seguenti norme (queste nuove normative dovrebbero sostituire in futuro i vari standard nazionali):
· la serie EN 50131 per i "sistemi di allarme antintrusione e antirapina".
Questa norma garantisce un alto livello di prestazioni sia per il consumatore che per il rivenditore, che può sfruttare la certificazione per promuovere il proprio prodotto.

Per i privati basta generalmente un grado 1 o 2.

PPer i negozi e le aziende sono più adatti i gradi 2 e 3 (rapporto rischio/investimento).
· la serie EN 50136 per i "sistemi e i dispositivi di trasmissione degli allarmi".
Questa norma riguarda i modelli di trasmissione a canale singolo e doppio, e determina con quali frequenze il polling deve essere configurato in base al tempo massimo di trasmissione accettabile.

In questo caso consiglio l'SP2/DP1 per i privati e il DP2/DP3 per i clienti aziendali.

Se hai domande o commenti contattami tramite e-mail, sarò lieto di rispondere al tuo messaggio:

pascal.hulalka@protectas.com

Protectas
Rue de Genève 70
1004 Lausanne

+41 21 623 26 00
swiss@protectas.com

www.protectas.com