Alberto Banzola (*)

Anelli di protezione: la difesa a strati delle infrastrutture critiche



Un data center, una centrale elettrica, uno scalo portuale hanno in comune una caratteristica poco visibile: quando si fermano, il danno non resta al loro interno. Si propaga a ospedali, circuiti di pagamento, trasporti, reti idriche. È l'effetto domino, ed è il motivo per cui si parla di infrastrutture critiche: sistemi la cui interruzione, anche breve, produce conseguenze sproporzionate rispetto alla loro estensione fisica.

(*) Sales Manager DEA Security **https://www.deasecurity.com/**

L'Unione europea ha preso atto di questa interdipendenza con la **Direttiva 2022/2557, detta CER** (Critical Entities Resilience), in vigore dal gennaio 2023 e recepita in Italia dal D.lgs. 134 del 4 settembre 2024. Il testo riguarda undici settori, dall'energia ai trasporti, dal credito alla sanità, dalle acque alle infrastrutture digitali. **Gli Stati devono individuare i «soggetti critici» e adeguarli ai nuovi obblighi di legge,** che comprendono una valutazione dei rischi naturali, tecnologici e dolosi da aggiornare almeno ogni quattro anni, un piano di resilienza, misure di sicurezza fisica adeguate, la continuità operativa e la notifica degli incidenti rilevanti entro 24 ore.

La difesa stratificata: gli anelli di protezione

Sul piano ingegneristico **la risposta è un principio ereditato dall'ambito militare: la difesa stratificata.** Nessuna barriera è infallibile, ma più barriere in serie aumentano il tempo che un intruso deve impiegare e le occasioni in cui può essere scoperto. Ogni «anello» svolge tre funzioni, dissuasione, rilevamento e risposta, e passa il testimone al successivo. La specifica tecnica europea CLC/TS 50661-1 formalizza questa impostazione parlando di «layer» della protezione.

> Dalla Direttiva CER alla fisica dei sensori: perché proteggere un sito essenziale significa scoprire l'intrusione prima che diventi effrazione.

Quattro anelli, dal confine ai varchi

Nella configurazione classica, che DEA Security - azienda italiana attiva dagli anni Settanta nei sensori perimetrali - articola in quattro livelli, **gli anelli sono concentrici. Il primo è la recinzione:** sensori applicati a rete o grigliato ne analizzano le vibrazioni per distinguere taglio, scavalcamento e sfondamento. **Il secondo è invisibile: nel terreno, a circa 60 centimetri, sensori geosismici piezoceramici** rilevano il passo di una persona o il transito di un veicolo. Non avendo elettronica attiva richiedono poca manutenzione, e l'intruso non sa dove sono. **Il terzo riguarda le pavimentazioni: sensori passivi annegati nel massetto** o sotto i pavimenti flottanti dei locali tecnici avvertono peso e movimento. **Il quarto è interno: rivelatori sismici di urti su infissi, pareti,** vetrate e mezzi forti che riconoscono la tecnica d'attacco. Colpi deboli e ripetuti suggeriscono uno scasso, un urto forte una rottura, una vibrazione continua un taglio o una foratura con utensili elettrici.

Il vero nemico: il falso allarme

Il problema più insidioso non è la mancata rilevazione, ma il falso allarme. Un sistema che scatta a ogni raffica di vento viene presto ignorato o disattivato, e un rilevatore ignorato è peggio di nessun rilevatore. Da qui la strada **della fusione di sensori:** i dispositivi più recenti, come quelli basati sulla tecnologia brevettata DEA Sensor Fusion, abbinano un trasduttore piezoelettrico, sensibile alle sollecitazioni meccaniche, a un accelerometro MEMS, sensibile a movimenti e accelerazioni, e confrontano i due segnali con algoritmi adattivi. L'evento diventa allarme solo se le due «testimonianze» concordano con la firma di un attacco. In un caso europeo, su 22 km di confine, la sostituzione di un sistema disturbato dalle condizioni atmosferiche ha ridotto sensibilmente i falsi positivi.

Dal sensore alla decisione

Rilevare non basta: **l'allarme deve trasformarsi in informazione utile. I sensori di nuova generazione dialogano via IP con piattaforme PSIM** (Physical Security Information Management), videosorveglianza, controllo accessi e sistemi di gestione dell'edificio, in modo da localizzare il punto esatto dell'evento e avviare procedure automatiche. Nel settore bancario, per esempio, centrali di allarme di grado 4 secondo la classificazione europea EN 50131 sono affiancate da sensori d'urto DEA di grado 3, con lo stato di infissi, casseforti e sportelli automatici visibile in tempo reale.

Resilienza, non adempimento

Un punto è centrale: la CER non è una lista di controllo da spuntare. La sicurezza fisica è la fondazione su cui poggiano continuità operativa, gestione delle crisi e, in coordinamento con le norme NIS2 e DORA, la dimensione cyber. E ciò che si misura, come il tempo medio di ripristino, si può migliorare. Un anello perimetrale da solo non basta; ma senza il primo anello, tutti gli altri entrano in gioco a intrusione già avvenuta.