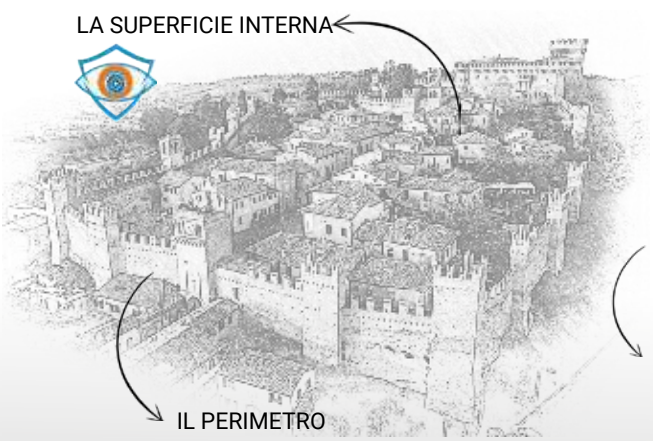

sicurezza proattiva **monitoraggio H24/7** **protezione conforme alla NIS2**

Cyber Fortress Model

Le nostre aziende devono diventare delle "fortezze digitali"

Le strategie del passato ispirano il modello di difesa e risposta al rischio informatico, di oggi e di domani.

I fatti parlano chiaro e delineano uno scenario sempre più allarmante: le aziende italiane, in particolare le PMI, sono sempre più bersaglio privilegiato della criminalità informatica. La sottovalutazione del rischio cyber, l'assenza di piani di continuità operativa e il fattore umano impreparato rendono le nostre aziende facili "prede" da colpire. E una PMI colpita non è solo una vittima diretta: spesso è anche la porta d'ingresso per attaccare realtà più grandi.

NESSUNA AZIENDA PUÒ RITENERSI AL SICURO

La protezione del proprio patrimonio digitale – dati, informazioni sensibili, risorse e know-how – dipende dalla capacità di adottare un approccio strutturato e continuo alla cyber security.
Oggi non è più sufficiente "difendersi" con un firewall o soluzioni temporanee. **Serve un cambio culturale** per costruire delle vere e proprie **"fortezze digitali" fondate** su un modello di difesa strutturato, all'altezza delle minacce di oggi sempre più subdole e sofisticate. Aspettare il danno per agire equivale, nella maggior parte dei casi, a non riuscire più a ripartire.

La difesa dipende dalla capacità di rilevare tempestivamente le minacce informatiche e bloccarle prima che sia troppo tardi.

DALLA FORTEZZA MEDIEVALE ALLA FORTEZZA DIGITALE

Il **Cyber Fortress Model OverRISK Suite, proposto dal Network Overlux®**, rilegge la sicurezza informatica con la logica del sistema di difesa delle fortezze medievali.
Il modello si articola su tre livelli: il perimetro, la superficie esterna e la superficie interna. Insieme costituiscono un **sistema di difesa proattiva basato su competenze, tecnologie, procedure e regole**.

IL PERIMETRO: RAFFORZARE LE "MURA DIGITALI"

Come le mura di un castello, il perimetro aziendale deve essere protetto con **firewall, antivirus e autenticazione multifattoriale**. Tuttavia, le sofisticate minacce di oggi riescono spesso ad aggirare queste difese, infiltrarsi nella rete e restare silenti per settimane prima di colpire (ransomware). Nasce, quindi, la necessità di attivare due ulteriori livelli di protezione: uno esterno e uno interno alla rete aziendale.

LA SUPERFICIE ESTERNA: PRESIDIARE IL DARK WEB

Nelle fortezze, sentinelle e informatori intercettavano le minac-

ce prima che raggiungessero le mura, attivando i piani difensivi. Oggi, fuori dalla rete aziendale, nel **dark web**, c'è un mercato illecito di dati rubati, utili a progettare **attacchi mirati e devastanti. Serve un "guardiano tecnologico" basato sulla threat intelligence per rilevare: attaccante, IP, CVE e modalità**. Ignorare ciò che accade fuori dal perimetro equivale a trascurare un nemico già alle porte, con le chiavi in mano.

LA SUPERFICIE INTERNA: RILEVARE E BLOCCARE LE MINACCE

Nella fortezza c'era un sistema per intercettare comportamenti sospetti e rispondere, secondo piani di difesa prestabiliti, a minacce entrate dentro le mura.
Anche oggi, nelle nostre reti, abbiamo le stesse necessità e il responsabile IT, da solo, non può affrontarle. **Occorre adottare un "guardiano interno", basato sulla threat intelligence, capace di rilevare e bloccare le minacce già penetrate**. Ma non basta la tecnologia: **serve un cambio culturale**. La sicurezza IT, infatti, è un dovere condiviso che parte dai vertici aziendali. **La NIS2 parla chiaro: gli organi di gestione devono guidare il cambiamento con consapevolezza e responsabilità**. La direttiva non è solo un obbligo normativo, ma un modello di governance per passare da un approccio reattivo a uno proattivo, fondamentale in un contesto di attacchi informatici sempre più diffusi e severi.

Le PMI possono innalzare da subito il livello di sicurezza con il KIT ROSSO di Overlux®.

Spesso ci dicono: "Costruire "LA FORTEZZA" richiede tempo. Come possiamo innalzare sin da subito la sicurezza aziendale?"

Sicuramente rafforzando la sicurezza perimetrale e attivando i "due guardiani" pronti a rilevare minacce e intervenire H24/7.
Un altro elemento chiave è l'attivazione del **SOC** (Security Operation Center), un team specializzato che analizza gli attacchi, individua le vulnerabilità sfruttate e fornisce supporto per la loro risoluzione.
Overlux® ha sviluppato **4 KIT** di cyber security, parte integrante della OverRISK Suite, utilizzabili singolarmente o in un percorso progettuale:

- BLU: censimento asset e monitoraggio connessioni
- GIALLO: gestione CVE software
- ARANCIONE: gestione e conservazione LOG
- ROSSO: OverLAN Guardian, OverDARK Guardian e SOC

Pensato per imprese di ogni dimensione e settore, il KIT ROSSO consente anche di adempiere agli obblighi NIS2 per soggetti essenziali e importanti, soprattutto nella gestione efficace e tempestiva degli incidenti.
I KIT servono a potenziare la difesa, attivare sistemi di monitoraggio continuo delle vulnerabilità e adottare misure H24/7 di risposta al rischio informatico.

COSTRUISCI IL TUO CYBER FORTRESS MODEL. Richiedi una prima consulenza gratuita a **commerciale@overlux.tech**