Italtel

CONFINDUSTRIA VENETO EST
Area Metropolitana
Venezia Padova Rovigo Treviso

NIS 2: Come prepararsi ai prossimi adempimenti

Proteggere il business
Monitoraggio e reazione come pilastri della cybersecurity aziendale

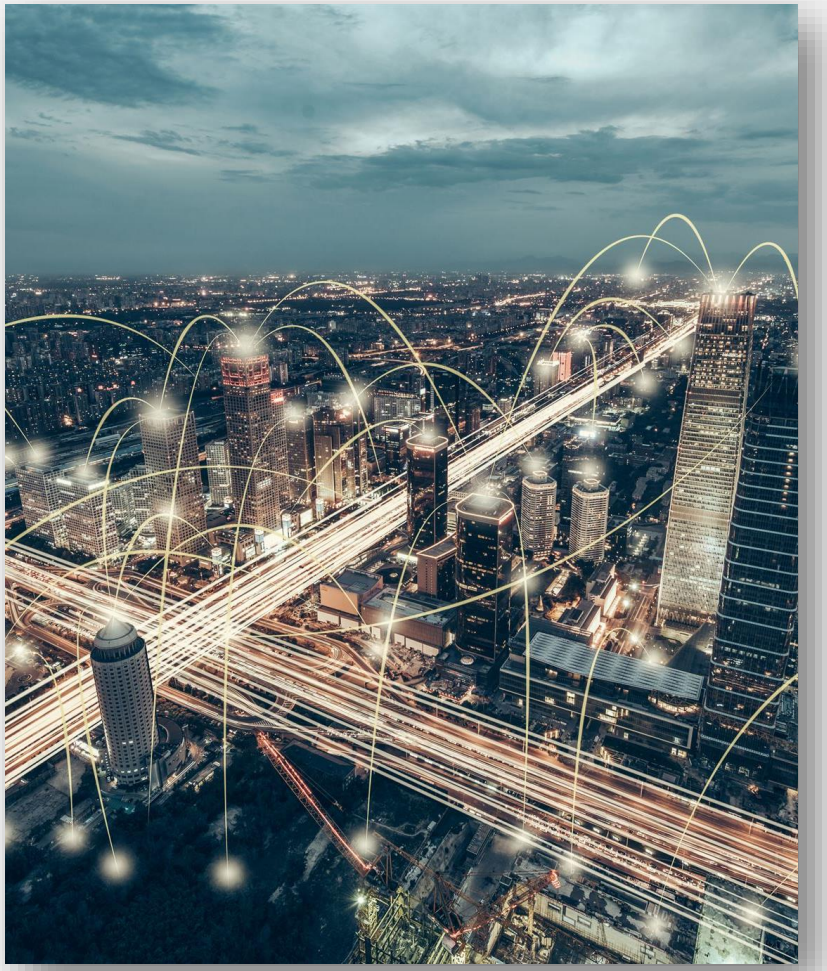
Milano, 11 novembre 2025

Ing. P. Allegra & Ing. D.G. Lucatti

AGENDA

- Protezione dati dalle minacce informatiche: trend e conseguenti impatti economico-reputazionali
- Tipologie di attacchi più comuni
- Primo pilastro – **Rilevare per proteggere**
- Secondo pilastro – **Reagire per contenere**
- Perché investire su questi servizi: continuità operativa e conformità normativa
- Esempi virtuosi e importanza della formazione
- **Quantum Security:** prevenire oggi le minacce di domani

Italtel nelle Industries e nella Cybersecurity



Ruolo di Italtel

- Storica società italiana, Italtel è un partner tecnologico chiave nelle telecomunicazioni e cybersecurity in Europa e America Latina.

Clienti e settori serviti

- Italtel fornisce soluzioni e servizi a principali operatori Telco e blue chips in varie industrie come trasporti, energia, banking e sanità.

Servizi di NOC, SOC & Cybersecurity

- Consulenza per assesment di cybersecurity e gestione delle vulnerabilità
- NOC multilingua e multi-national H24
- Monitoraggio e reazione agli incidenti per le reti ICT.

Requisiti Direttiva NIS2 per la sicurezza informatica

Approccio strutturato alla gestione del rischio

- La Direttiva NIS2 impone un metodo organizzato per identificare e gestire i rischi cibernetici.

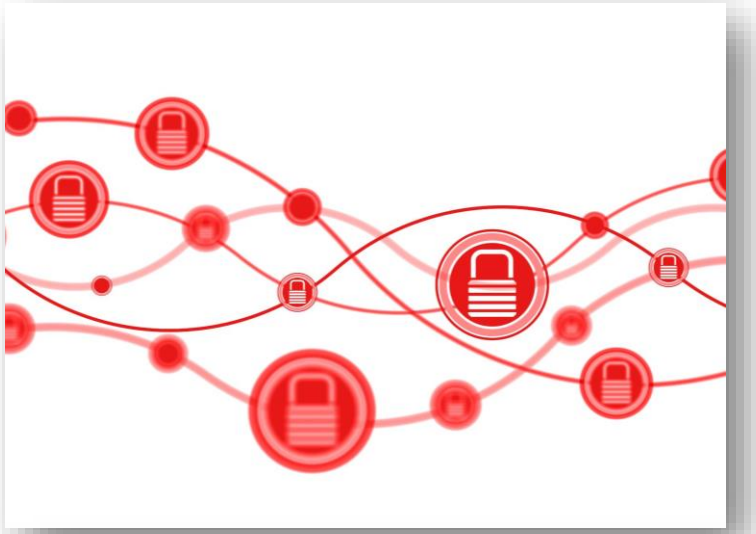
Conoscenza del livello di esposizione

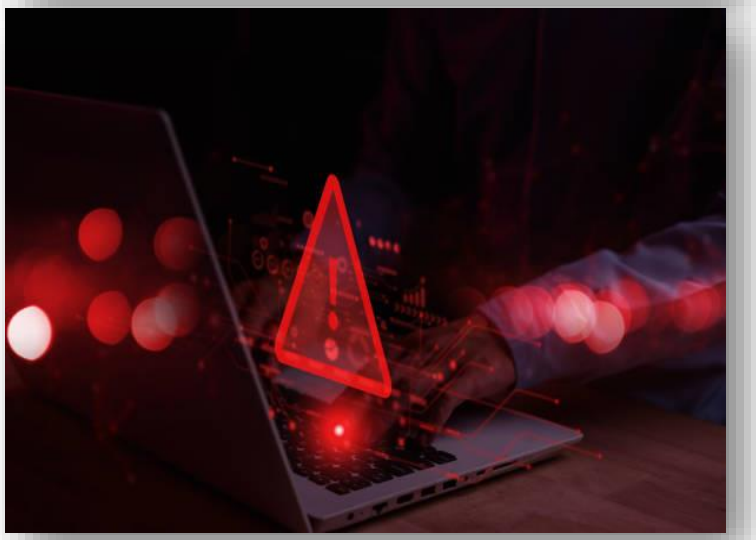
- Le organizzazioni devono valutare accuratamente la propria esposizione ai rischi informatici.

Misure di sicurezza adeguate e documentate

- È necessario implementare misure di sicurezza proporzionate, efficaci e formalmente documentate.

Caso Reale: Attacco Ransomware e Gestione della crisi





Attacco ransomware

- Nel settembre 2023 un hacker ha penetrato la rete aziendale di una multinazionale italiana nella categoria 1000-5000 dipendenti ed ha cifrato i dati con un virus ransomware, bloccando l'accesso.

Profilo aziendale e dipendenti

- L'azienda era una società tecnologica con dipendenti prevalentemente di estrazione tecnica che utilizzavano PC e rete informativa.

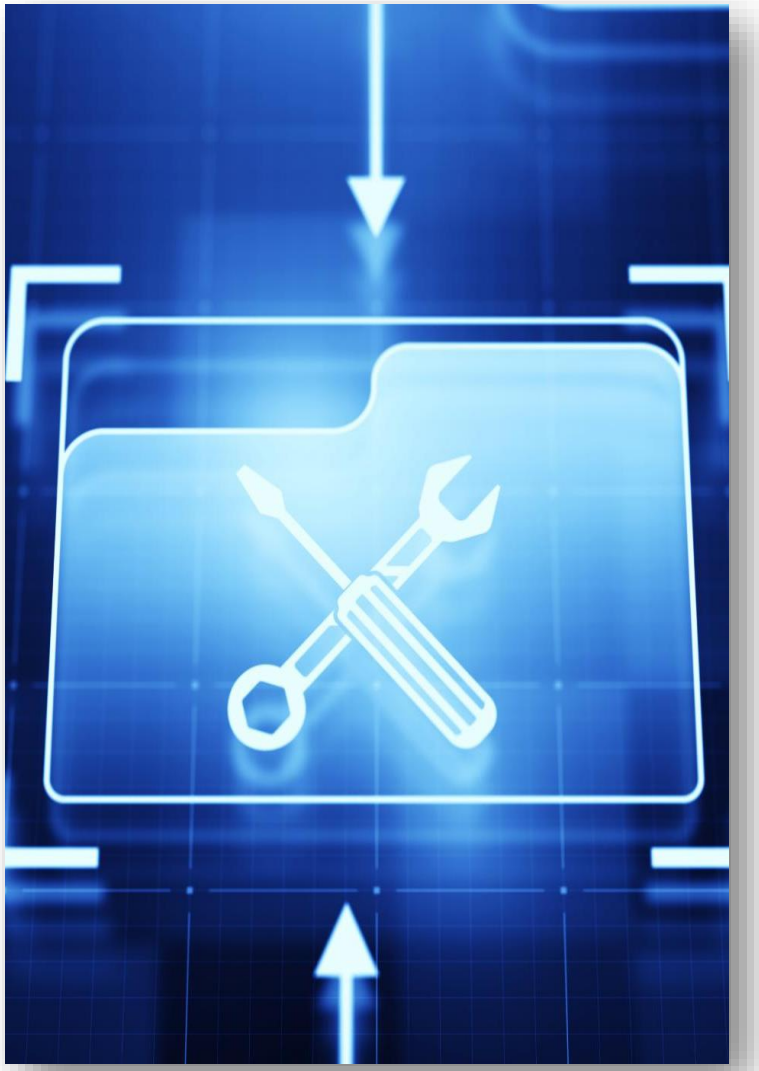
Infrastruttura IT aziendale

- La rete dati comprendeva centinaia di nodi, migliaia di PC, Data Center on premise e servizi Cloud interconnessi.

Misure di sicurezza implementate

- La rete era ben protetta con firewall, VPN, DMZ, controllo accessi e gestione identità per la sicurezza informatica.

Caso Reale: Recupero tramite backup e conseguenze operative



Recupero dati con backup

- Il Disaster recovery ha permesso di evitare il pagamento del riscatto recuperando tutti i dati compromessi con una copia di backup adeguata.

Processo di sicurezza post-attacco

- È stato necessario aggiornare sistemi operativi, antivirus e riformattare macchine, server e laptop per garantire la sicurezza e l'operatività della rete.

Riconfigurazione e ripristino operativo

- Le macchine sono state riconfigurate una per una e l'ultimo backup sano è stato ricaricato per ristabilire la piena operatività.

Caso Reale: 4 Impatti

1) Blocco operativo e ripresa

- L'operatività aziendale fu completamente bloccata per settimane con ripresa graduale dopo un mese e mezzo.

2) Gestione organizzativa e strategia

- Necessario richiamare tutti i laptop e progettare una strategia per la bonifica e reinserimento progressivo in rete.

3) Impatto economico elevato

- Il fermo operativo di circa un mese ha causato costi elevati per l’azienda, tra fermi e riavvii delle applicazioni.

4) Danno reputazionale e comunicazioni

- L’azienda dovette informare Autorità e parti interessate del potenziale furto dati, mitigando il danno reputazionale.

Analisi delle principali cause e vulnerabilità

Complessità della superficie di attacco

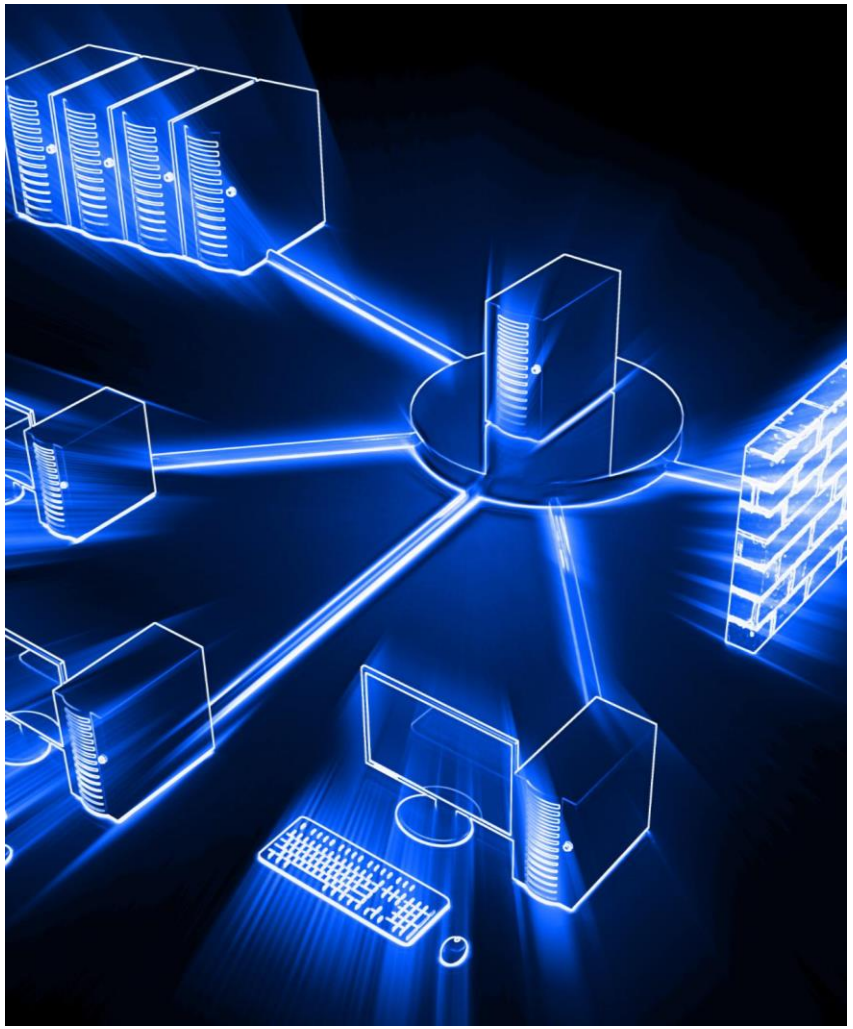
- La rete moderna è distribuita e difficile da proteggere, con accessi da remoto e infrastrutture cloud e on-premises.

Variabile umana e sicurezza

- Gli utenti remoti e l’autenticazione multi-fattore introducono variabilità e rischi nella sicurezza della rete.

Nuove vulnerabilità emergenti

- Le applicazioni web e B2B espongono nuove superfici di attacco che richiedono analisi specialistiche continue.



Ruolo della variabile umana e tecniche di spear phishing

Imprevedibilità della variabile umana

- La variabile umana è il punto più imprevedibile e difficile da controllare nella sicurezza aziendale.

Tecniche di Spear Phishing

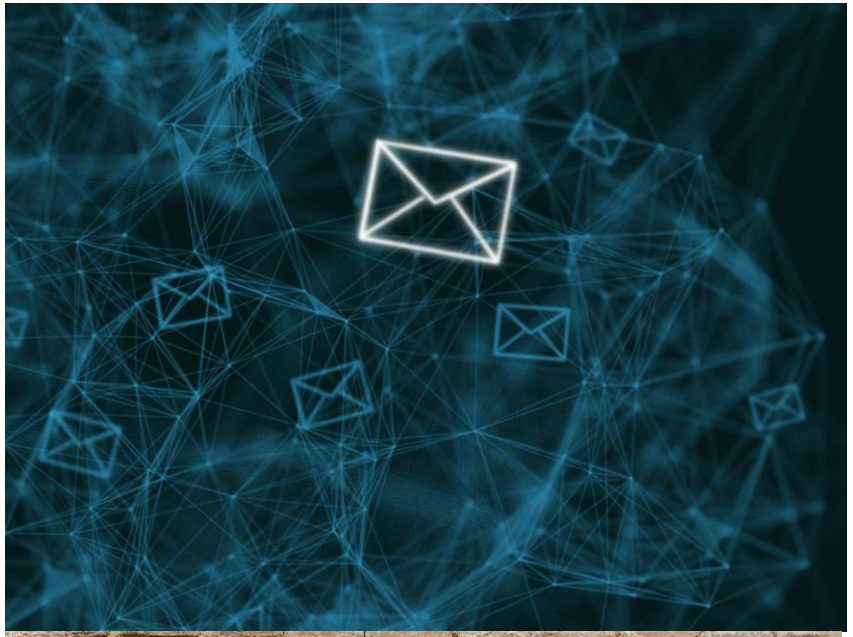
- Gli attacchi spear phishing usano informazioni raccolte dai social per ingannare la vittima con email personalizzate e realistiche.

Protezione oltre le difese tradizionali

- Oltre a difese fisiche, è necessario un monitoraggio continuo per rilevare aperture involontarie o violazioni.

Adeguamento costante delle reti

- Le reti aziendali sono in continua evoluzione e richiedono aggiornamenti per mantenere elevata la sicurezza.



Nuove vulnerabilità e importanza della Cyber Threat Intelligence

Nuove vulnerabilità zero-day

- Le vulnerabilità zero-day emergono continuamente, rendendo le reti inizialmente sicure, vulnerabili rapidamente.

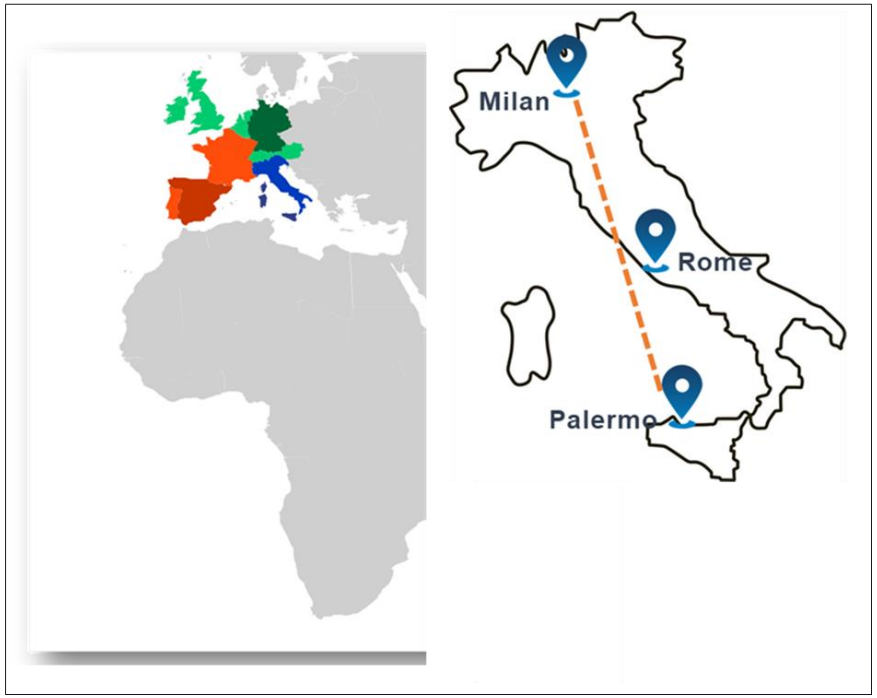
Importanza degli aggiornamenti software

- Gli aggiornamenti e le patch di sicurezza sono essenziali per mantenere efficaci le difese contro le nuove minacce.

Ruolo della Cyber Threat Intelligence

- La Cyber Threat Intelligence monitora siti fasulli, password trafugate e fornisce alert per difese tempestive.

DIGITAL OPERATION CENTER
L’importanza della presenza Multinazionale e Multilingua



Importanza della presenza internazionale

- Sempre di più le aziende Italiane hanno business e relazioni in Europa ma anche in altri continenti

Multilingua

- Oltre l’Italiano anche Inglese, Spagnolo e Portoghese

DIGITAL OPERATION CENTER
Il valore aggiunto del servizio SOC 24 x7

ITIL | ISO 9001 | ISO 27001 | ISO 20000-1 | ISO 22301

Importanza del servizio SOC

- Il servizio SOC è fondamentale per un approccio organizzato e strutturato alla gestione del rischio informatico.

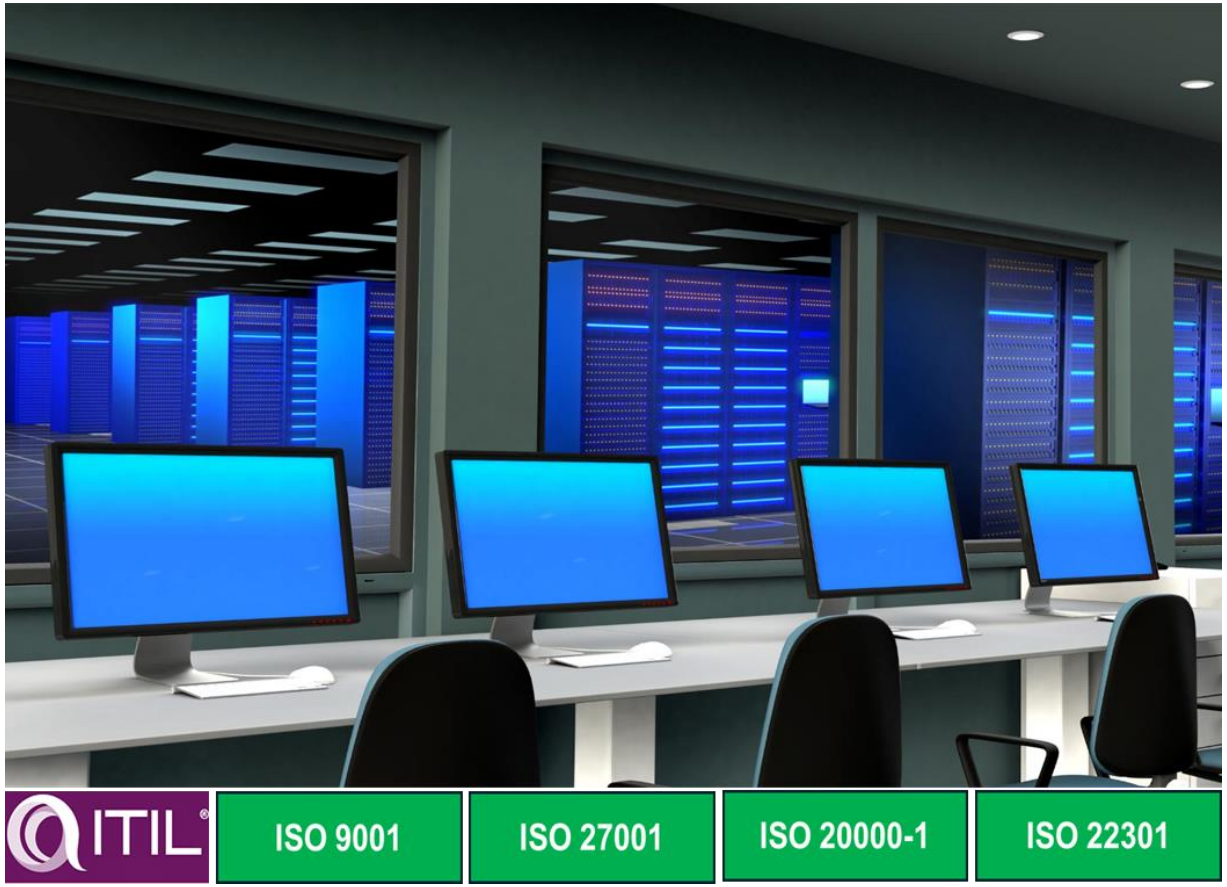
Gestione del rischio cyber

- Il SOC consente di identificare, analizzare e rispondere efficacemente alle minacce informatiche in tempo reale.

Esperienza pratica

- L'esperienza diretta nel campo della consulenza ingegneristica sottolinea il valore strategico del SOC nella protezione aziendale.

Monitoraggio continuo e risposta agli incidenti: MDR



Monitoraggio continuo SOC

- Il SOC opera 24 ore al giorno per monitorare da remoto l'infrastruttura IT e intercettare eventi di sicurezza rilevanti.

Attività di Detection

- La Detection consiste nell'identificare tempestivamente ogni evento significativo per la sicurezza informatica.

Risposta agli incidenti

- La Response attua azioni immediate per respingere, mitigare e rimuovere attacchi informatici dall'infrastruttura.

Ricostruzione e prevenzione

- Si ricostruisce la dinamica dell'attacco per implementare misure correttive e ridurre il rischio futuro.

Esempio pratico di Detection & Response

Rilevazione dell'anomalia

- Il SOC identifica accessi sospetti da paesi remoti non autorizzati e sessioni multiple simultanee.

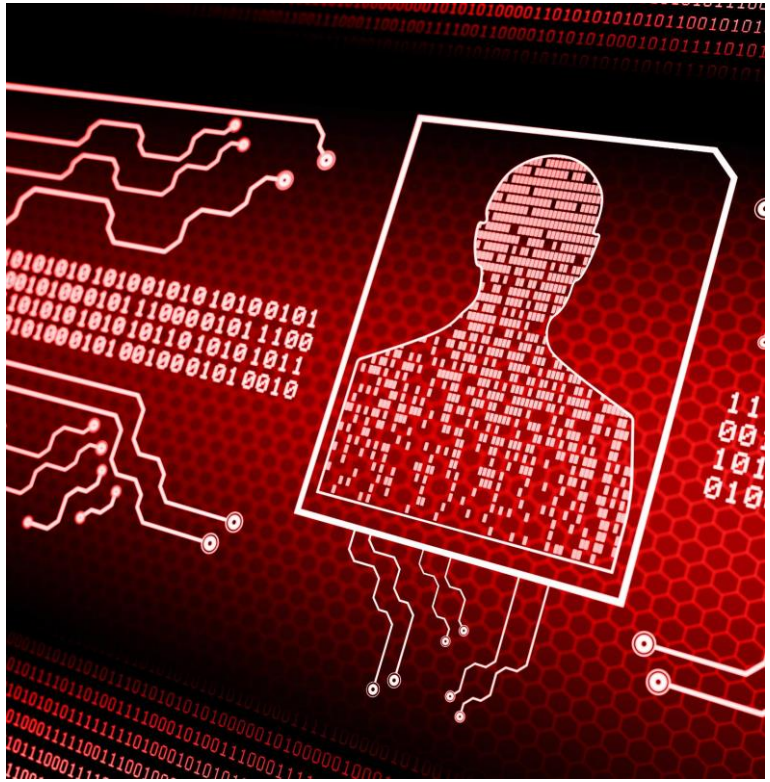
Correlazione degli eventi

- Il SOC collega link malevoli ricevuti con successivi inserimenti di credenziali compromesse.

Azione di risposta rapida

- Il SOC revoca la sessione compromessa, resetta la password e avvisa l’utente telefonicamente.

Tecniche di attacco informatico più comuni



Attacco tramite phishing

- Il phishing è la prima fase di attacco per ingannare l'utente e ottenere credenziali di accesso sensibili.

Intercettazione Man in The Middle

- L'attacco Man in The Middle intercetta l'autenticazione a più fattori compromettendo la sicurezza MFA.

Movimento laterale nella rete

- L'hacker utilizza il movimento laterale per spostarsi attraverso la rete, oltrepassando firewall e sistemi di sicurezza.

Compromissione di server e dati

- Una volta dentro, l'attaccante accede a server e database critici per rubare o criptare dati aziendali.

Principali tipologie di attacco: malware, phishing, DDoS, exploit, SQL injection

Malware e Ransomware

- Il malware, incluso il ransomware, rappresenta una minaccia crescente con famiglie come Warlock, Babuk e Kraken.

Phishing e Whaling

- Il phishing, inclusa la variante Whaling rivolta ai dirigenti, è una tecnica sofisticata di inganno via email.

Attacchi DDoS

- Gli attacchi DDoS mirano a sovraccaricare i sistemi, causando interruzioni significative dei servizi online.

Exploit e SQL Injection

- Gli exploit zero-day e le iniezioni SQL sfruttano vulnerabilità per accedere o manipolare dati sensibili.

Le tre componenti di un SOC efficace

Tecnologia: strumenti, piattaforme e automazione

Strumenti e piattaforme software

- SIEM, XDR e sistemi di protezione email rilevano e correlano eventi sospetti generando allarmi per gli operatori.

Automazione con architetture SOAR

- Automatizzare le risposte permette reazioni immediate e riduce la propagazione di minacce in rete.

Ruolo dell’intelligenza artificiale

- L’IA supporta il SOC migliorando la velocità di reazione, sempre sotto supervisione umana competente.

Competenze degli operatori SOC e gestione degli allarmi

Filtraggio e correlazione eventi

- Operatori SOC filtrano e correlano milioni di eventi per identificare minacce reali e ridurre i falsi positivi.

Gestione falsi positivi

- Gli operatori scremano falsi allarmi per evitare interventi inutili, concentrandosi su minacce significative.

Risposta agli attacchi

- In caso di attacco confermato, gli operatori mitigano l’impatto evitando il blocco totale dell’azienda.

Processi organizzativi: runbook, playbook e procedure di escalation

Analisi Forense e Gravità Incidente

- L’analisi forense determina rapidamente la gravità dell’incidente e la necessità di notifica obbligatoria entro 24 ore.

Criteri di Classificazione Incidenti

- È fondamentale bilanciare la classificazione per evitare falsi allarmi che non hanno impatto significativo reale.

Runbook e Playbook Procedurizzati

- I runbook e playbook definiscono sequenze di interventi chiari per ogni possibile attacco, riducendo improvvisazioni.

Matrici di Escalation e Comunicazione

- Le procedure includono matrici di escalation tecnica e manageriale, oltre a piani di comunicazione con clienti e specialisti.

Formazione del personale e simulazioni di phishing

… 4

Importanza della formazione

- La formazione del personale è essenziale per rafforzare la difesa contro attacchi informatici, specialmente quelli basati sull'inganno.

Riconoscere gli elementi di rischio

- I dipendenti devono imparare a identificare mittenti sospetti, link pericolosi e documenti non sicuri per evitare rischi.

Hardenig dei dispositivi

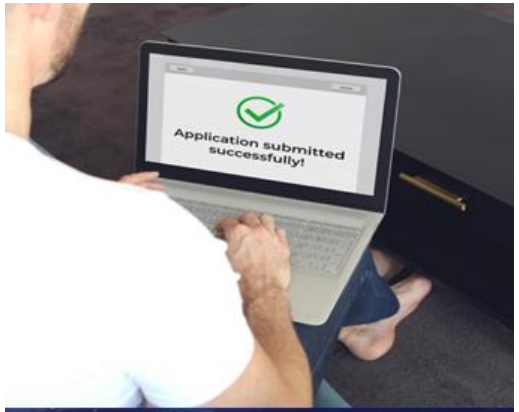
- Proteggere l'utente dalle operazioni ad elevato rischio mediante opportuna configurazione e gestioni dei dispositivi aziendali.

Simulazioni di phishing

- Le campagne di phishing simulate testano la sensibilità e l'attenzione del personale verso email malevole.

Applicazione del principio ‘Need2Know' e procedure aziendali

… 5



Principio del Need to Know

- Garantire che i dipendenti accedano solo ai dati indispensabili per il loro ruolo, limitando l'accesso a informazioni sensibili.

Procedure di autorizzazione rigorose

- Implementare processi di autorizzazione che non si basano su semplici email, ma includono verifiche telefoniche o sistemi di autorizzazione digitale.

Prevenzione delle vulnerabilità

- Evitare procedure che permettano operazioni sensibili non verificate, riducendo i rischi di attacchi hacker.

Quantum safe/secure: Priorità Minacce e Regulatory

Regulatory Compliance

2

3

Market is adjusting to new conditions

Harvest-now decrypt-later attacks

1

4

Clock is ticking

Gov/Defense → Critical Infrastructure → Regulated Enterprise → General Enterprise → Consumers

Sector

Stack Layer

Different layers have different complexity

Gartner Tech Trend # 4) Postquantum Cryptography Quantum computing advancements will render current encryption standards unsafe by 2029, necessitating a shift to post-quantum cryptography.

La Tecnologia è pronta…

Distributed Symmetric Key Exchange (DSKE)

Based on pre-placed random data

PROs: provably safe, cost-effective.

CONs: requires out-of-band delivery of random data (PSRD).

Quantum Key Distribution (QKD)

Based on quantum mechanics

PROs: provably safe, identifies intruders *before* the communication happens.

CONs: limited range, expensive; does not achieve the reach of software-based methods AS IS infrastructure. PKI based networks Difficult to upgrade using QKD
.

Post-Quantum Cryptography (PQC)

Based on asymmetric encryption algorithms, standardized by NIST

PROs: software based, cost-effective.

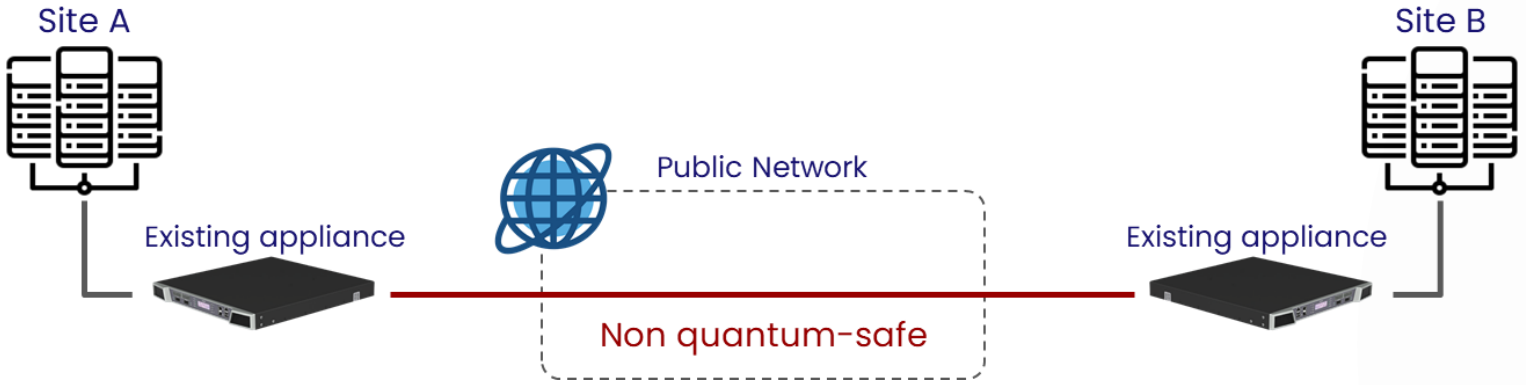
CONs: Not provably safe against conventional or quantum computers, computationally expensive.

Distributed Symmetric Key Exchange (DSKE) advantages:

- **30+% lower deployment cost** vs. QKD systems
- **Fully software-defined approach** – no need for dedicated fiber or proprietary hardware
- **Minimal CAPEX & OPEX**: leverages existing optical/IP networks and SW orchestration/automation centralized
- Enhances **brand trust** and customer retention in regulated industries (Finance, Defense, Energy)

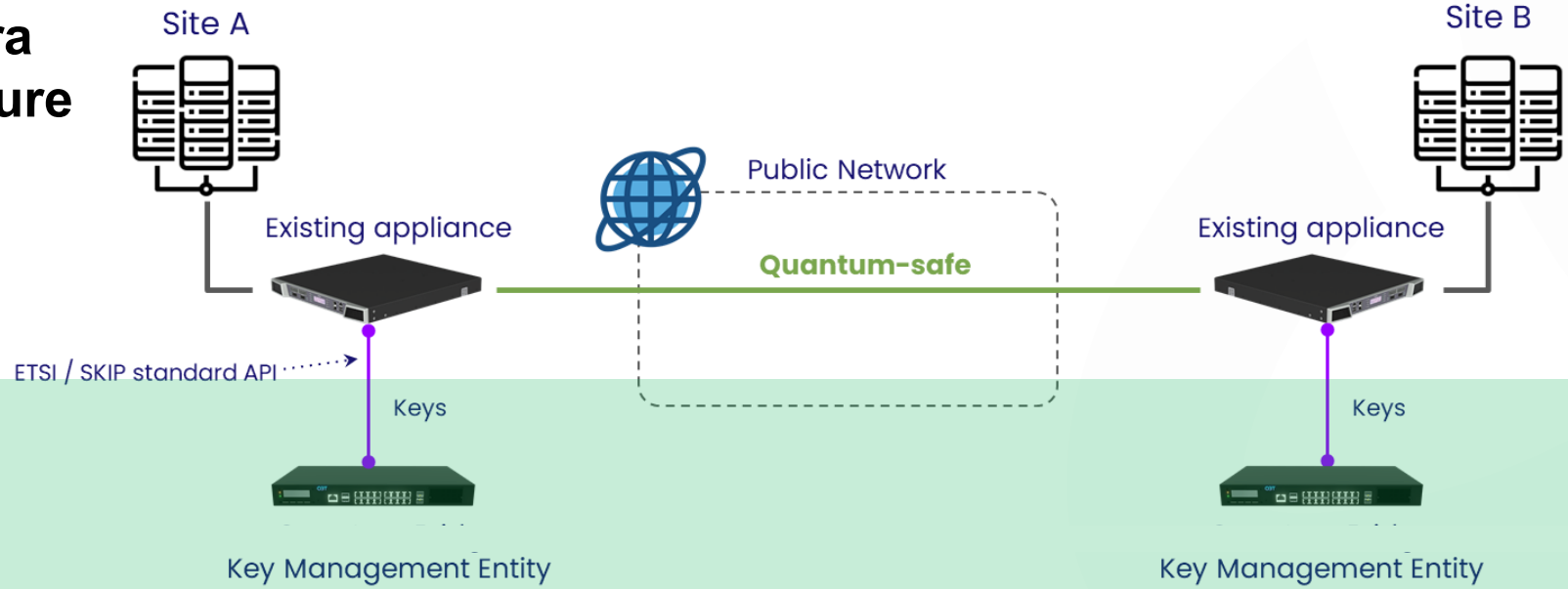
… e si può implementare in modo facile

Tipica Infrastruttura Non Quantum Safe



Nuova Infrastruttura Quantum safe & secure

- **KME**
- **SECURITY HUB**



Conclusioni

- **La sicurezza informatica è una priorità strategica**: fondamentale per affrontare le sfide moderne e proteggere sistemi e dati critici.
- **SOC efficace come pilastro**: il Servizio SOC di Italtel integra tecnologia avanzata e competenze specialistiche per una risposta tempestiva e strutturata agli incidenti.
- **Integrazione di tecnologia, processi e formazione**: la combinazione di strumenti innovativi, procedure organizzative e formazione continua garantisce la continuità operativa e la resilienza aziendale.

- **Adattamento alle nuove minacce**: l'evoluzione delle minacce (es. ransomware, phishing, vulnerabilità zero-day) richiede aggiornamenti costanti, Cyber Threat Intelligence e simulazioni di attacco.
- **Verso la Quantum Security**: prepararsi oggi alle sfide di domani adottando soluzioni post-quantum e strategie di crypto-agility per la protezione a lungo termine.

Contatti

Riferimento commerciale

- **Ing. Dario G. Lucatti**
  Chief Business Development Officer
  dariogiuseppe.lucatti@italtel.com
  M: +39 348 8067373

Riferimento tecnologico

Ing. Paolo Allegra
Chief Global Unit Officer
paolo.allegra@italtel.com
M: +39 335 7251558

Italtel S.p.A.
Via Caldera, 21
20153 Milano MI - Italy

Italtel

Grazie

LEGAL NOTICE: