3ª EDIZIONE

CYBERSEC 2024

ROMA, ITALIA

LA CYBERSECURITY NELL'ERA DELL'AI
INFRASTRUTTURE CRITICHE, IL CASO DELLA RISORSA IDRICA

6-7 MARZO

www.cybersecitalia.events

CYBERSECURITY ITALIA EVENT

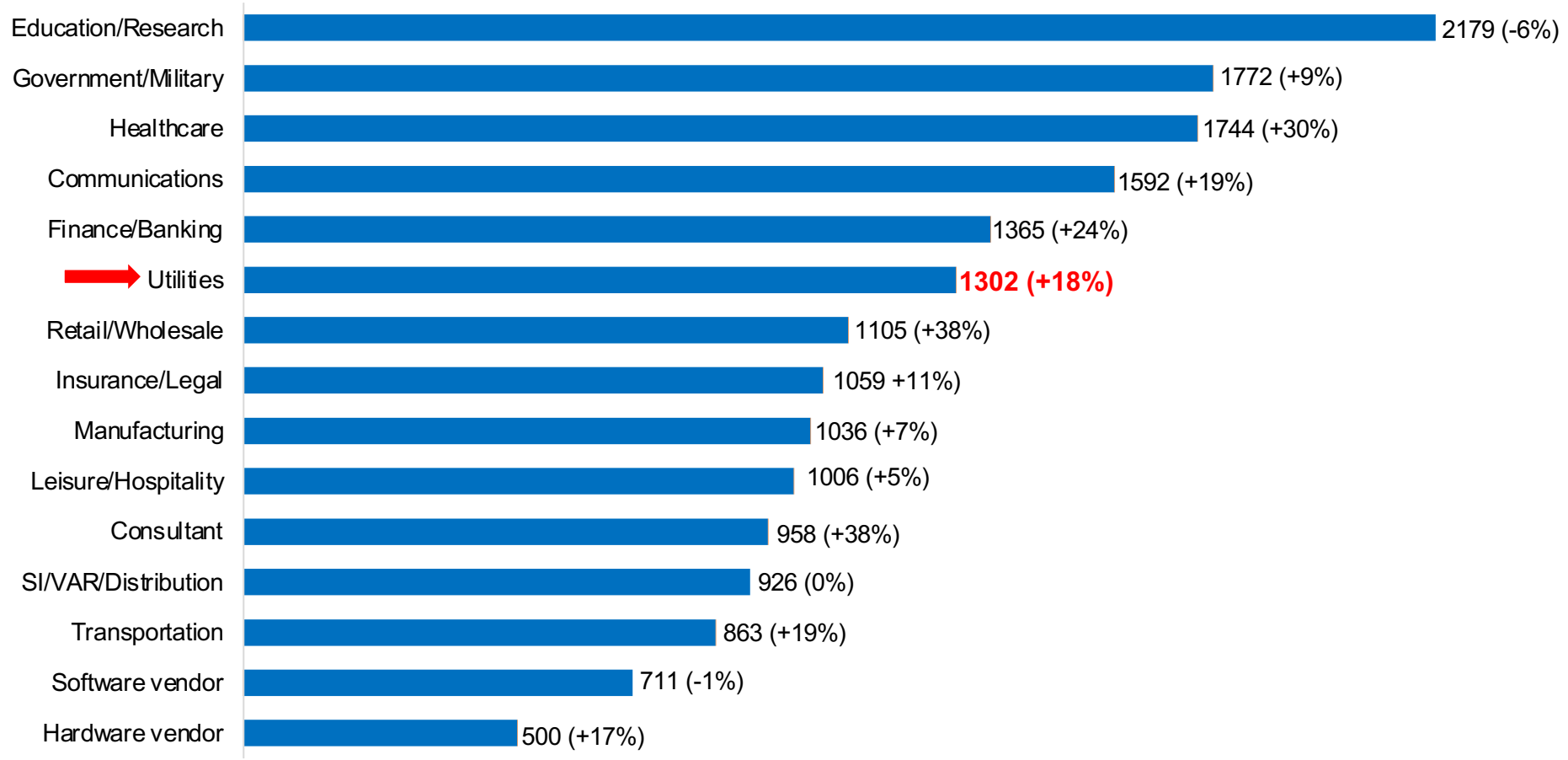
CYBERSECURITYITALIA

RELATORE

ROGER CATALDI

***CISO**, Almaviva*

Tendenza degli attacchi informatici Global Avg. Weekly Cyber Attacks per Industry 2023 Q2 vs 2022 Q2



** Riferimento Check Point Research (CPR), 2023*

Impatto di alcuni attacchi informatici del 2023

Al momento, le infrastrutture critiche in Italia subiscono attacchi di tipo opportunistico, che non mostrano i segni di una regia unificata o di attacchi coordinati (es. State-Sposored).

Primaria Multi Utility Nazionale, 2023

Primaria Utility Regionale, 2023

Consorzio di Bonifica Nazionale, 11/2023

Impianti di trattamento delle acque in Israele, 11/2023

La minaccia di azioni State-Sponsored

Soprattutto nell'attuale contesto internazionale di instabilità geopolitica, cresce la preoccupazione verso **cyber attacchi terroristici**, che potrebbero avere l'intento di bloccare i servizi essenziali di città, regioni e interi paesi.

- Attacchi informatici State-Sponsored contro obiettivi strategici come mezzo di coercizione politica ed economica.
- Attacchi mirati al sistema idrico che potrebbero causare effetti a catena con impatti drammatici sulla società e sulla nostra economia.

Quali rischi si corrono

Questi sono alcuni fra i primari rischi associati alle minacce informatiche che possono mettere in ginocchio le infrastrutture critiche idriche.

- Interruzione dell'approvvigionamento idrico
- Compromissione della qualità dell'acqua
- Inquinamento delle acque reflue
- Danneggiamento delle infrastrutture critiche
- Compromissione dei sistemi di monitoraggio
- Compromissione della Safety
- Danni reputazionali e perdita di fiducia
- Furto e compromissione dei dati
- Violazioni normative/legali

Direttiva NIS2

- Valutazione rischi e Gestione crisi
- Aggiornamento di sistemi e applicazioni
- Formazione del personale
- Collaborazione con le autorità competenti
- **Sicurezza della Supply Chain**
- Crittografia
- Autenticazione a più fattori
- Obbligo 1° notifica incidenti entro 24h

Aspetti sanzionatori

I **Soggetti Essenziali** non conformi, rischiano sanzioni pari a un massimo di almeno **10 milioni di EUR o pari al 2% del totale del fatturato** mondiale annuo dell'impresa di appartenenza, se tale importo è superiore.

I **soggetti Importanti** non conformi, rischiano sanzioni pari a un massimo di almeno **7 milioni di EUR o all'1,4% del totale del fatturato** mondiale annuo dell'impresa di appartenenza, se tale importo è superiore.

DIFENDERSI E' POSSIBILE

È possibile ridurre l'esposizione al rischio utilizzando i servizi di Intelligence offerti da Almaviva tramite il suo Cyber Threat Defence Center, conformi alle normative e alle linee guida del settore OT, come la serie IEC 62443

Best practice di sicurezza

- Valutazione del rischio
- Classificazione dei sistemi e dei dati
- Controlli di accesso
- Segmentazione della rete
- Difesa in profondità
- Monitoraggio continuo
- Aggiornamenti e patch
- Formazione del personale
- Test di sicurezza e Audit
- Piani di ripristino

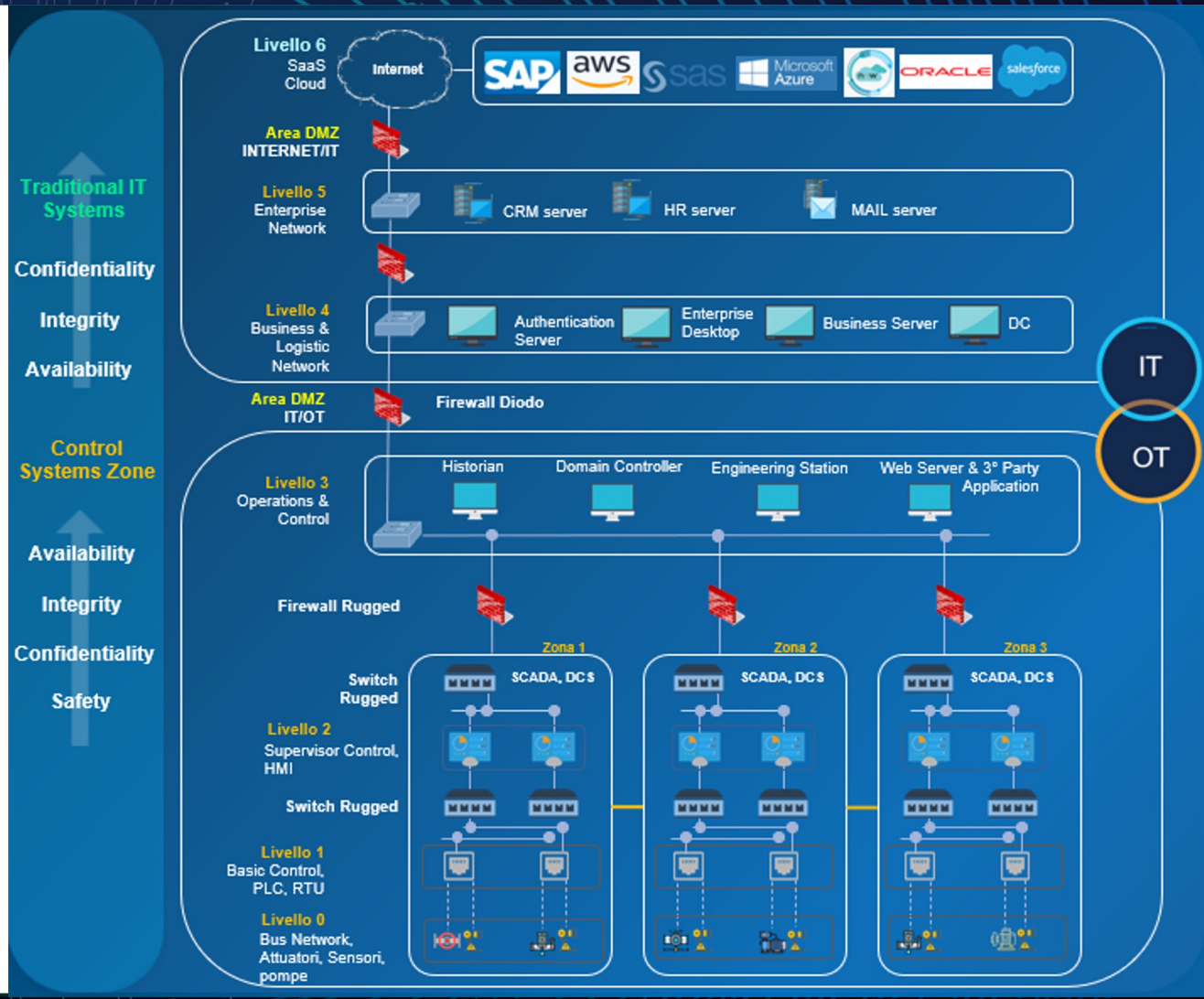
Standard IEC 62443

Framework internazionale per la sicurezza dei sistemi di controllo industriale (ICS) e sistemi critici.

Lo standard copre diversi aspetti della sicurezza operativa:

- Valutazione del rischio
- Protezione dei dati
- Controllo accessi
- Segmentazione della rete
- Monitoraggio delle minacce
- Procedure di risposta agli incidenti di sicurezza

- ICS Monitoring
- Privileged Access Management (PAM)
- Fixed Function Security
- Passive Security Assessment
- Software Security Assessment - VA
- Software Security Assessment – PT
- Software Security Assessment Code Review
- Hardware Security Assessment
- Red Teaming



Piattaforme di simulazione degli scenari

Sviluppare **scenari di simulazione degli attacchi informatici** alle infrastrutture critiche.

Esempi di scenari di simulazione

- Interruzione dell'acqua in aree critiche.
- Contaminazione delle risorse idriche.

Caratteristiche di una piattaforma di simulazione

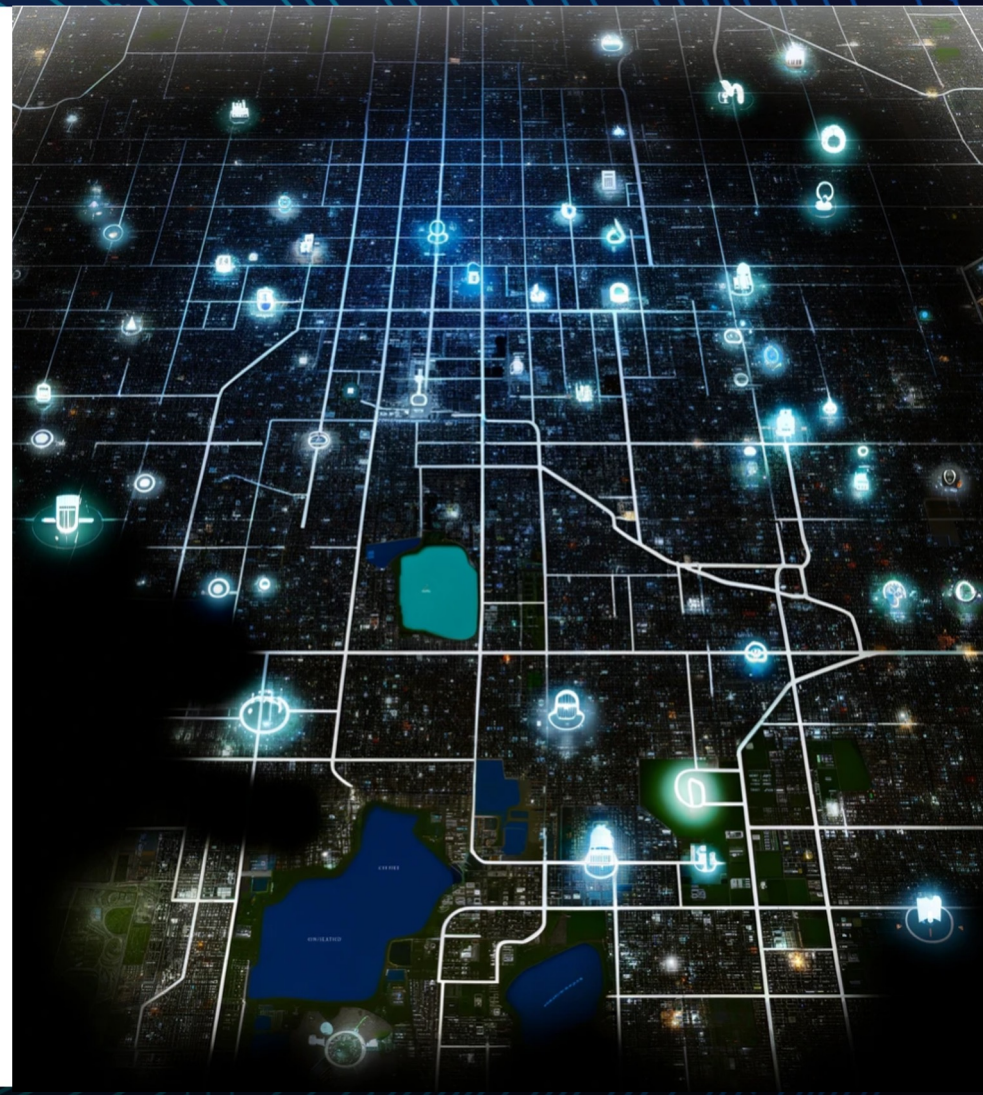
- Personalizzazione degli scenari (incorporando specifiche variabili).
- Simulazione e valutazione di impatto con analisi dettagliata delle conseguenze.

Applicazioni pratiche

- Test delle contromisure per valutazione dell'efficacia.
- Coinvolgimento multidisciplinare (enti governativi, operatori di settore ed esperti di cybersecurity).

Benefici primari

- Maggiore resilienza.
- Miglioramento della capacità di risposta.



Almaviva

Grazie

presales.cybersecurity@almaviva.it