Palazzo Altieri - Roma, 27/03/2025

DORA -> ITAM
I RIFLESSI DEL REGOLAMENTO SULLA SICUREZZA FISICA BANCARIA

DR. NILS FAZZINI
CHIEF STRATEGY AND SALES BDS S.p.A.

Base Digitale

BASE DIGITALE NEL GRUPPO

Sesa

Innovazione Tecnologica e
Digital Services
per il mercato business

(1) Ricavi e Risorse Umane FY April 30, 2024E

Base Digitale

DORA

Direttiva CER
Direttiva (UE) 2022/2557

resilienza dei soggetti critici il Consiglio dei ministri del 7 agosto 2024 ne ha approvato, in esame definitivo, i decreti legislativi di attuazione

Direttiva NIS2
Direttiva (UE) 2022/2555

recepita dai singoli Stati membri UE entro il 17 ottobre 2024 pertanto il Consiglio dei ministri del 7 agosto 2024 ne ha approvato, in esame definitivo, i decreti legislativi di attuazione

Cybersecurity Act - CSA
Regolamento (UE) 2019/881

Relativo all'ENISA, l'Agenzia dell'Unione europea per la cybersicurezza, e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cybersicurezza»)

Cyber Resilience Act
(in corso di definizione)

proposta di regolamento sui requisiti di sicurezza informatica per i prodotti con elementi digitali

Dora
Regolamento (UE) 2022/2554

Applicabile dal 17 gennaio 2025 DORA (Digital Operational Resilience Act) è una normativa che mira a garantire un elevato livello di resilienza operativa digitale per il settore finanziario

Direttiva E-privacy Direttiva 2002/58/CE

Attuata in Italia con Dlgs 196/2003

Data Governance Act
Regolamento (EU) 2022/868

Relativo alla Governance europea dei dati che modifica il regolamento (UE) 2018/1724 (Regolamento sulla governance dei dati)

GDPR
Regolamento (UE) 2016/679

DSA- Digital Services Act
Regolamento (UE) 2022/2065

DMA- Digital Markets Act
Regolamento (UE) 2022/1925

EIDAS
Regolamento (UE) n. 910/2014

NORMATIVE E REGOLAMENTI CYBERSECURITY

NORMATIVE E REGOLAMENTI CONTIGUI ALLA CYBERSECURITY

BDS

ITAM

Coerentemente con le Normative in vigore, quali DORA, NIS2 e IEC62443, l'IT Asset Management (ITAM) rappresenta il processo più utile per aiutare le banche nel gestire nel modo corretto il ciclo di vita dei device IT e IOT e rispondere alle esigenze di compliance e audit correlato.

In cosa consiste un processo del genere:

- La discovery «agentless», per poter dare un riscontro alle aziende del reale parco IT/IoT/Sicurezza fisica per poter evidenziare gli asset aziendali catalogandoli, mettendo in evidenza eventuali asset non desiderati e/o non gestiti; i dati rilevati aggiornano il CMDB aziendale.
- Il servizio di Early Warning , la verifica del patching dei dispositivi, per evidenziare eventuali asset non conformi con firmware e/o sistemi operativi «out of date»
- Il patching automatizzato, dei dispositivi, con workflow autorizzativo
- La gestione dei change e del decommissioning dei dispositivi
- L'assistenza proattiva , da remoto ed on-site a copertura e completamento del servizio.

Deve essere integrato/integrabile con le tecnologie già eventualmente presenti di asset management, Asset discovery, ITOM, ITSM, Monitoring, Digital Twin, Unified End Point Management ed altri….

BDS

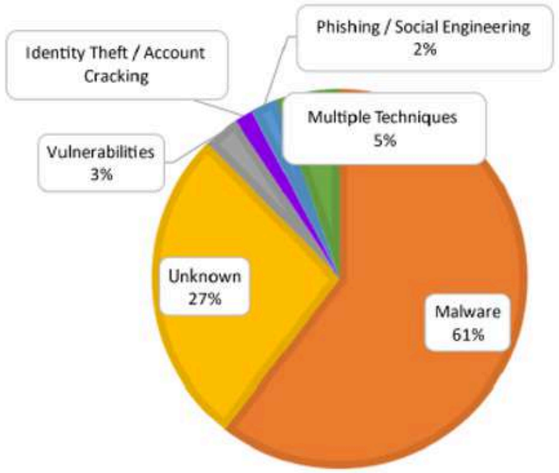
IL CONTESTO

ESTRATTO RAPPORTO CLUSIT 2023 UPDATE OTTOBRE 2023
Un'Asset non aggiornato determina il 47% degli attacchi CyberCrime

Rapporto Clusit 2023 sulla sicurezza ICT in Italia

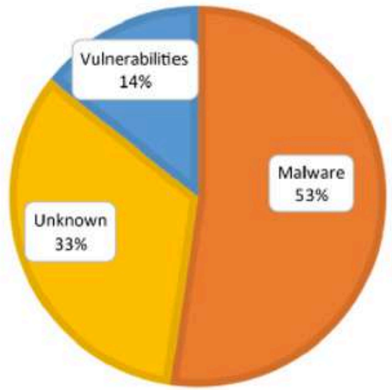
Il Malware (nello specifico ransomware) che rimane oltre il 50% anche nel 2023, Data Breach (indicati come tecnica "unknown") e Vulnerabilità (in particolare 0-day) sono le tecniche di attacco più sfruttate. Da notare il trend in aumento dello sfruttamento delle Vulnerabilità nel 2023.

MANUFACTURING PER TECNICA 2022



© Clusit - Rapporto 2023 sulla Sicurezza ICT in Italia

MANUFACTURING PER TECNICA 1H 2023



© Clusit - Rapporto 2023 sulla Sicurezza ICT in Italia

L'Europa è il continente più attaccato, arrivando a coprire il 50% degli attacchi verso il settore nei primi 6 mesi del 2023. Segue l'America, una minoranza di attacchi verso l'Asia e pochissimi verso location multiple. (Da valutare meglio la consistenza dei numeri relativi ad attacchi nel "Rest Of the World", ovvero Asia, Oceania, Africa che risultano poco rappresentativi).

Quasi il 50% delle principali minacce in ambito Manifatturiero sono determinati da asset non inventariati o da aggiornamenti di sicurezza mancanti, con una crescita rispetto al 2022 maggiore del 50% !

BDS

LA NECESSITA'

L'analisi del rischio informatico è un aspetto fondamentale per la gestione del ciclo di vita del sistema informativo, necessaria per poter effettuare una fotografia dell'as-is e comprendere eventuali strategie da applicare

Avere la mappatura degli asset informatici è fondamentale, con informazioni fresche ed aggiornate, motivo per il quale devono essere identificati e classificati in base alla loro importanza per l'azienda.

Possiamo categorizzare gli asset in queste macrocategorie

- Microinformatica
- network e security
- IoT
- Sicurezza fisica

Per poter mappare gli asset dobbiamo necessariamente «rilevarli» in modo automatico ed in modalità agentless.

Tecnologie, competenze, certificazioni e expertise sono alla base per poter erogare un servizio proattivo e governato per raggiungere questo fondamentale scopo e le linee guida dettate dalle normative (**IEC62443**) ci danne le linee guida di cosa e come gestire gli asset ed i relativi rischi.

BDS

layout concettuale

PSIM

Physical Security/O.T.

Network security

Informatica distribuita

Mobile & Rugged

Discovery

Patching

ORCHESTRAZIONE - AUTOMAZIONE - DASHBOARD

IT SERVICE MANAGEMENT

Service Desk - H24

PATCHING

REQUEST

INCIDENT

BDS

Vantaggi e Benefici

(per i security manager delle banche)

Creare un’effettiva testa di ponte tra sicurezza fisica e logica

Adeguare il parco tecnologico

Investire sul salto evolutivo prossimo della sicurezza fisica -> DPA/AI

Automatizzare i processi di manutenzione preventiva del parco

Ridurre la superficie di attacco dovuto al scarsa manutenzione informatica dei device di campo

BDS

BDS

Connect with us.

BDS S.p.A.
Via Leonardo da Vinci,20
50132 FIRENZE

www.basedigitalegroup.com

infobds@basedigitalegroup.com

+39 055 907 3699

+39 055 907 3600