La quinta colonna, come prevenire l'attacco interno

Intervento presso il Master di 1° livello in Cybersecurity

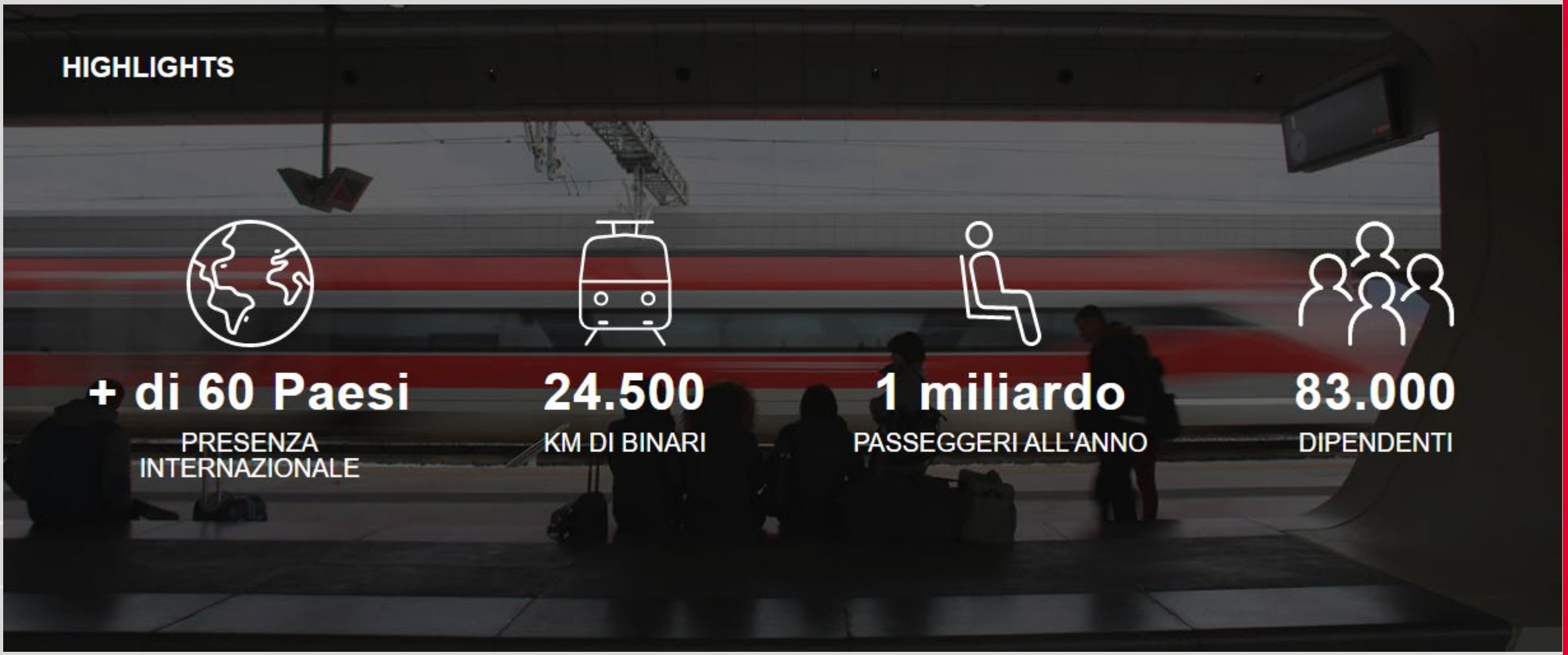
Giorgio Aprile

Data Protection Officer Ferrovie dello Stato Italiane SpA

24 luglio 2020

FERROVIE DELLO STATO ITALIANE

Il Gruppo Ferrovie dello Stato



INDICE

Attacchi esterni vs attacchi interni

Una veloce panoramica

Il più importante data breach del secolo

WikiLeaks ha svelato ai quotidiani New York Times e The Guardian e al settimanale tedesco Der Spiegel il contenuto di alcuni documenti riservati dai quali emergono aspetti nascosti della guerra in Afghanistan. Tra le altre cose, le suddette informazioni riguardano: l'uccisione di civili e l'occultamento dei loro cadaveri; l'esistenza di un'unità segreta americana dedita a "fermare o uccidere" talebani, anche senza un regolare processo; il doppio gioco del Pakistan — ufficialmente paese alleato degli Stati Uniti — i cui servizi segreti tessevano rapporti di collaborazione con i capi talebani per combattere l'operato militare statunitense e organizzare perfino complotti contro capi afghani …


The New York Times

Hackers Tell the Story of the Twitter Attack From the Inside

Several people involved in the events that took down Twitter this week spoke with The Times, giving the first account of what happened as a pursuit of Bitcoin spun out of control.

Il più recente attacco hacker

The enormous Twitter hack that led to the accounts of a former US president, a possible future president, numerous billionaire businessmen, celebrities and the world's most valuable company all promoting a bitcoin scam may go down as one of the worst cybersecurity disasters ever to hit a social media company.
But while the scope of the incident was massive in its own right — impacting accounts belonging to Barack Obama, Joe Biden, Bill Gates, Elon Musk, Kanye West, Kim Kardashian West and Warren Buffett — it could merely be the tip of a very large iceberg with vast security implications. Cybersecurity experts and policymakers now worry that the bitcoin scam may mask a much more troubling data breach involving the personal communications of the world's most powerful people.

Attacchi esterni vs attacchi interni

Definizioni e probabilità di successo

Si definisce attacco interno quello in cui è coinvolto almeno un dipendente del soggetto attaccato o almeno un dipendente di un fornitore del soggetto attaccato, aventi accesso ai sistemi informativi di quest'ultimo.

A Clark School study at the University of Maryland is one of the first to quantify the near-constant rate of hacker attacks of computers with Internet access— every 39 seconds on average

In 2018, of the 5 billion records stolen/ compromised, over 2 billion were a result of insider circumstances[1]

More than 50% of companies had a confirmed insider attack in the past 12 months[2]

Attacchi Esterni

- Numeri elevatissimi
- Bassa probabilità di successo
- Impatto "generalmente" limitato
- Spesso poco sofisticati
- …

Attacchi Interni

- Numeri bassi
- Alta probabilità di successo
- Impatto "generalmente" alto
- Spesso piuttosto sofisticati
- …

1. Risk Based Security, Inc. Data Breach QuickView Report, Year End 2018 - Data Breach Trends. Includes malicious and accidental circumstances
2. 2. Crowd Research Partners: 2018 Insider Threat Report

Attacchi esterni vs attacchi interni

Indicatori di Rischio

97% of insider threat cases studied by Stanford University involved an employee whose behavior a supervisor had flagged, but that the organization had failed to follow up on.

92% of insider threat cases were preceded by a negative work event, such as a termination, demotion, or dispute with a supervisor.

90% of IT employees indicate that if they lost their jobs, they'd take sensitive company data with them.

59% of employees who leave an organization voluntarily or involuntarily say they take sensitive data with them.

51% of employees involved in an insider threat incident had a history of violating IT security policies leading up to the incident.

25% of employees have used email to exfiltrate sensitive data from an organization.

Network Activity
- Excessively large downloads
- Access request denials

Compliance Cases
- Noncompliance with training requirements
- Policy violations

Data Exfiltration
- Spikes in outbound email traffic volume
- Attachments sent to suspicious recipients
- Removable media alerts

Time & Expense
- Expense violations
- Time entry violations

Access Attributes & Behaviors
- Access levels
- Security clearances
- Privileged user rights

Personnel Management
- Declining performance reviews
- Notice of resignation or termination
- Disciplinary action

Physical Security
- Physical access request denials
- Physical access anomalies

External Data
- Social media posts
- Financial duress
- Criminal/civil history
- Foreign contacts/travel

Source: "Insider threats: What every government agency should know and do," Deloitte Dbriefs, March 2016.

INDICE

Il principio del "need to know" e la gestione delle utenze

È molto rischioso che tutti sappiano tutto …

- Per principio di *"need to know"* si intende la limitazione degli accessi e dei coni di visibilità ai soli soggetti che ne necessitano al fine di svolgere un determinato task
- Collegato al concetto precedente, ma con alcune differenze, è il principio del *"least privilege"*, che consiste nella massima limitazione dei privilegi rilasciati a ciascun soggetto alle utenze *"machine to machine"*
- L'applicazione dei due principi implica una chiara consapevolezza di cosa risiede sui sistemi e la classificazione delle informazioni

UNA RIGOROSA GESTIONE DELLE UTENZE

Il principio del "need to know" e la gestione delle utenze

Classificazione NATO …

- COSMIC TOP SECRET (CTS) - This security classification is applied to information the unauthorized disclosure of which would cause exceptionally grave damage to NATO. (NOTE: The marking "COSMIC" is applied to TOP SECRET material to signify that it is the property of NATO. The term "NATO TOP SECRET" is not used.)
- NATO SECRET (NS) - This security classification is applied to information the unauthorized disclosure of which would cause serious damage to NATO.
- NATO CONFIDENTIAL (NC) - This security classification is applied to information the unauthorized disclosure of which would be damaging to the interests of NATO.
- NATO RESTRICTED (NR) - This security classification is applied to information the unauthorized disclosure of which would be disadvantageous to the interests of NATO.

Il principio del "need to know" e la gestione delle utenze

La gestione delle utenze è un'attività complessa

- È necessaria una mappatura delle applicazioni
- È necessaria un'analisi funzionale per stabilire chi deve vedere cosa, i cd coni di visibilità
- La stessa analisi deve identificare le azioni che ogni utente dell'applicazione può e non può effettuare (download, queries, estrazioni report, stampe …)
- È necessario implementare un collegamento all'anagrafica aziendale e ai sistemi di *"identity management"* per bloccare le utenze in caso di cambio ruolo (o pensionamento …)
- È necessario un workflow autorizzativo che contenga dei passaggi periodici per la verifica della persistenza delle necessità di accesso
- È necessario un controllo periodico delle utenze che non effettuano accessi (se un utente non effettua accessi per più di 3 mesi, probabilmente non ha bisogno delle credenziali di accesso)

Relativamente semplice se ci si pensa in fase di progettazione (Data Protection by Design)

Molto più complesso per sistemi esistenti

Il principio del "need to know" e la gestione delle utenze

Il tasso di "infedeltà" è più o meno costante …

Molti Data Breach (soprattutto quelli che fanno male), partono da soggetti che hanno un accesso autorizzato ai sistemi

INDICE

Il tracciamento delle attività

La certezza di essere scoperti è un forte deterrente …

- Il log delle operazioni può essere logicamente distinto su due classi:
  - Log infrastrutturali e tecnici
  - Log applicativi
- I log infrastrutturali e tecnici sono collegati all'architettura utilizzata, non sono customizzabili (diciamo poco customizzabili) e non sono sufficienti a tracciare le operazioni svolte sulle applicazioni
- I log applicativi sono riferiti all'applicazione e, per le applicazioni più recenti, consentono un tracciamento puntuale delle operazioni svolte dagli utenti, sia ordinari che quelli con ampi privilegi:
  - Accesso e uscita (il minimo indispensabile)
  - Operazioni sui dati (quali ad esempio queries, modifiche, cancellazioni)
  - Download massivi
  - Stampe
  - Etc…
- Sui log applicativi è possibile costruire triggers per l'attivazione di allarmi

Il tracciamento delle attività

Forensic vs Real Time

FORENSIC

- Il log devono essere inalterabili
- I log devono essere conservati per un tempo sufficiente (almeno 6 mesi, suggeriti i 12)
- I log devono essere pertinenti, leggibili e facilmente analizzabili

REAL TIME

- Ridurre al minimo la dimensione dei log (information overflow)
- Stabilire i comportamenti anomali (serve anche per addestrare sistemi AI) determinando i trigger. È necessaria la cooperazione delle funzioni di business
- Collegare tutto al SIEM …

Il tracciamento delle attività

Utenti ordinari delle applicazioni vs utenti con privilegi ampi

Utenti Ordinari

- Tutti gli utenti di un'applicazione rappresentano una minaccia
- Attenzione a comportamenti ripetuti nel tempo
- Attenzione ai tentativi di accesso a funzionalità superiori e all'utilizzo di credenziali diverse

Amministratori di Sistema e "SuperUsers"

- Rappresentano gli utenti più rischiosi in quanto dotati di privilegi ampi
- Va monitorato tutto
- Attenzione ai cd SuperUsers, utenti formalmente non nominati come AdS ma con ampi privilegi per il download e le modifiche

INDICE

La normativa di riferimento e le cautele da utilizzare

Ma si può fare?

General Data Protection Regulation

- Necessità di realizzare un Data Protection Impact Assessment

Statuto dei Lavoratori

- Valutare accordi sindacali

Grazie