**Attacchi Cyber**

*Tempo stimato*: 10’

*Obiettivi di apprendimento*

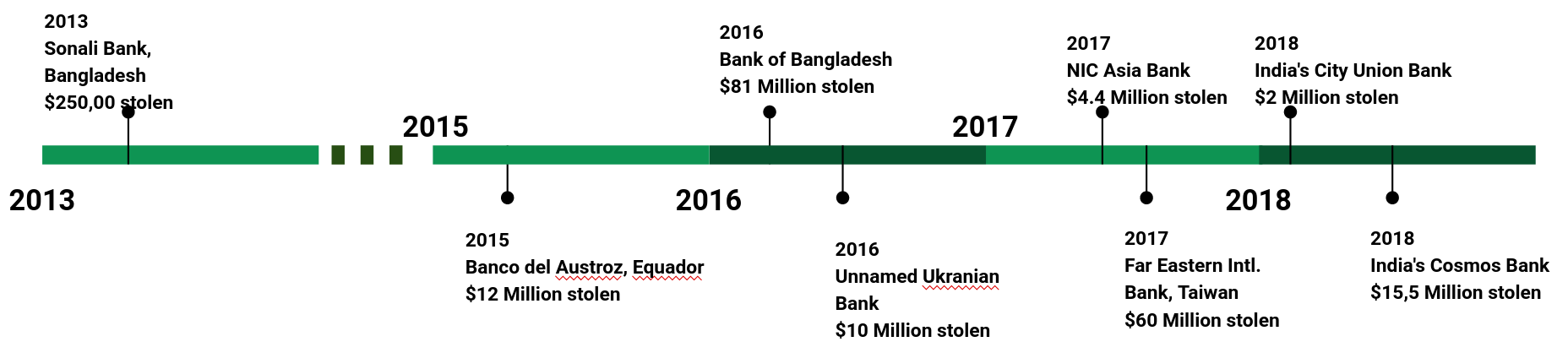
Alla fine di questa sezione sarai in grado di

* valutare la portata degli attacchi cyber

Gli attacchi cyber sono ormai riportati con cadenza quasi quotidiana dai *mass media.* A trovare spazio sui giornali sono spesso gli attacchi a operatori di infrastrutture critiche (ad es. le aziende di produzione e/o distribuzione di energia elettrica, gas, acqua), le infrastrutture finanziarie (ad es. le banche), o i servizi governativi. Ciò non significa che le altre tipologie di organizzazioni (ad esempio di minor dimensione o operanti in altri settori) siano meno esposte alla cyber-risk. Gli attacchi cyber colpiscono tanto le le organizzazioni governative quanto le aziende e l’esposizione alla minaccia non dipende dalla dimensione o dal settore in cui opera l’organizzazione. In altre parole, nessuna organizzazione moderna può ritenersi immune agli attacchi cyber, ovvero non soggetta a cyber-risk.

Nel 2017 ben tre diversi attacchi su larga scala (WannaCry, Petya, NotPetya) sono stati realizzati utilizzando **ransomware**, ovvero una particolare tipologia di malware progettata per penetrare nelle infrastrutture informatiche della vittima, produrre disservizi quali la cifratura dei patrimonio informativo e richiedere il pagamento di un riscatto in Bitcoin per rientrare nella disponibilità dei dati cifrati. Questi attacchi hanno colpito un’ampia varietà di organizzazioni (agenzie governative, fornitori di servizi di pubblica utilità, ospedali) situate in diversi paesi. Mentre l’obiettivo più immediato di questi attacchi è apparentemente il guadagno economico, ci sono ragioni per pensare che l’intento degli attacchi sia stato anche quello di colpire l’operatività delle organizzazioni vittima facendo in tal modo pensare ad uno stato-nazione quale agente ostile.

Nel lasso di tempo che va dal 2013 al 2017, almeno 8 attacchi di alto profilo hanno colpito SWIFT, ovvero l’infrastruttura informatica utilizzata nel mondo da più di 11.000 istituzioni finanziarie per condurre transazioni. Gli attacchi, condotti da gruppi criminali molto ben organizzati, hanno portato complessivamente alla sottrazione illecita di più di 160 milioni di dollari. In questo caso gli attaccanti hanno sfruttato non tanto vulnerabilità nei sistemi informatici quanto quelli presenti nelle procedure e nei processi delle istituzioni finanziarie vittime dell’attacco.

Figura 1. - Attacchi a SWIFT

Altri gruppi di criminali cyber si sono invece focalizzati sulle singole banche, alterandone i bilanci al fine di accreditare ingenti somme di denaro sui conti correnti nelle loro disponibilità, oppure -- in modo ancor più eclatante -- sovvertendo il funzionamento degli sportelli automatici in modo tale da consentire l’illecito prelievo di denaro da parte di loro complici. Si stima che il danno economico complessivo causato da questi attacchi si aggiri sul miliardo di euro. Questi attacchi, denominati *Advanced Persistent Threat (APT)*, sono caratterizzati dalla capacità degli attaccanti di penetrare l’infrastruttura informatica della vittima sfruttando vulnerabilità dell’infrastruttura informatica e l’involontaria partecipazione dei dipendenti della banca (mediante tecniche di *social engineering*) e di mantenere in essa la propria presenza senza essere notati anche per lunghi periodi di tempo (in alcuni casi anche per mesi) durante i quali gli attaccanti identificano le vulnerabilità nelle procedure e nei processi aziendali e sviluppano tecniche di attacco specifiche.

L’esfiltrazione o l’alterazione di dati sensibili custoditi dalle organizzazioni (ad es. informazioni anagrafiche, numeri di carta di credito, dati sanitari) è un obiettivo spesso perseguito dagli attaccanti cyber. Si pensi che nel **Dark Web** (ovvero in quella porzione del web dove, grazie a tecnologie che consentono navigazione e pagamenti con garanzia di anonimato, esiste un fiorente commercio di beni e servizi illegali) è possibile acquistare (in modo ovviamente illegale) dati sanitari ad un costo che attualmente oscilla tra i 250 e i 1.000 dollari per individuo. L’attacco condotto recentemente al sito dei pagamenti della *American Medical Collection Agency (AMCA)*, un’azienda di esazione dei crediti di operatori sanitari ha portato all’esfiltrazione di dati sensibili (nome, numero di previdenza sociale, l’indirizzo di residenza, data di nascita e numero della carta di credito) di più 20 milioni di cittadini americani. Oltre al costo diretto causato dalla gestione dell’incidente informatico, il danno reputazionale è stato così ingente da portare l’azienda al fallimento.