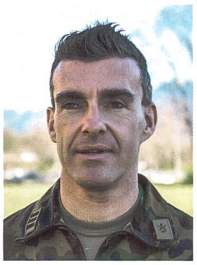
Zeitschrift: Rivista Militare Svizzera di lingua italiana : RMSI
Herausgeber: Associazione Rivista Militare Svizzera di lingua italiana
Band: 91 (2019)
Heft: 4

Artikel: Asimmetrie, tecnologia e fattore umano nei rischi cibernetici
Autor: Annovazzi, Mattia
DOI: https://doi.org/10.5169/seals-867886

Asimmetrie, tecnologia e fattore umano nei rischi cibernetici

Il rischio crescente di attacchi informatici e gli strumenti per contrastarli efficacemente sono stati al centro del quarto *Private Banking Day*, tenutosi il 17 maggio 2019 scorso al KKL di Lucerna.



col
Mattia Annovazzi

colonnello Mattia Annovazzi

Esperti di alto profilo hanno illustrato le sfide in ambito globale e nazionale e presentato i rischi concreti, ma anche le opportunità, per la Svizzera e la sua piazza finanziaria.

Di particolare interesse è stato l'intervento di Assaf Mischari, già componente del cyber-command delle forze armate israeliane e attuale direttore della ricerca della startup *Team 8*, attiva nel campo della cibersicurezza.
Ha focalizzato il suo intervento sulla cibercriminalità, vista dalla parte di chi attacca uno specifico soggetto economico, statale o istituzionale (*Fit the target*). In questo caso si tratta anche di un modello di business: c'è chi crea un prodotto (ad esempio un *bot*), chi lo vende, chi lo usa; c'è un *aftermarket*, ci sono licenze vendute e servizi di supporto di regola più efficaci e disponibili rispetto a quelli offerti per la protezione da attacchi.

L'asimmetria tra attaccante e parte attaccata

Se da un lato, poche persone "proattive" con pochi mezzi possono portare attacchi efficaci senza particolari ostacoli, d'altro lato chi difende è legato a un contesto complesso, rigido, vulnerabile, costoso e regolamentato e viene posto di regola nelle condizioni di poter soltanto reagire. Il rischio di venir scoperti e sanzionati per l'autore è considerevolmente basso. Non esiste un "prezzo per il fallimento": si possono tentare attacchi ad esempio con un *malaware* in modo indisturbato, fino a quando si riesce. Le sempre maggiori regolamentazioni e standardizzazioni su controlli, compliance e *best practices* hanno reso prevedibile – e quindi pericoloso – il comportamento degli utenti e le modalità di gestione dei rischi. Stessi strumenti e modalità di operare, significano ad esempio che se si scopre un modo per accedere ai sistemi di una banca, verosimilmente potrò accedere a tutte le banche più o meno allo stesso modo. Si tratta di un'ulteriore asimmetria in favore dell'attaccante.

Come procede un hacker?

L'attaccante cercherà dapprima di comprendere quale sia il *comportamento normale* nella gestione di dati, di sistemi, di reti ecc. Ma cosa vuol dire normale? Difficile definirlo. Ci si basa, ad esempio, su comportamenti dannosi di dipendenti scoperti in passato e sui meccanismi di protezione realizzati di conseguenza.
In un secondo momento, l'attaccante cerca di comprendere quali siano le *anomalie* del sistema. Un'azione su 10 000 sembra, statisticamente, essere considerata come veramente malevole e dannosa per un sistema. Significa che lo specialista potrebbe trovarsi confrontato con un attacco dannoso per ogni 10 000 allarmi pervenuti.
Infine, si tratta di capire *cosa vuole ottenere* un ciberattaccante. Vuole soltanto accedere a un computer? Vuole

informazioni su un software, su un prodotto? Vuole sottrarre dati e informazioni? Cercherà di operare in modo simile a quanto fanno i dipendenti e gli operatori di un'organizzazione, in modo da non essere rilevato da allarmi di sistema. Attacchi sofisticati includono anche quelli ai responsabili IT.

Che forma può assumere un attacco?

L'accesso a una rete, secondo il relatore, è relativamente semplice; basta trovare una persona che commetta un errore di manipolazione, attraverso un click o un doppio click, ad esempio su un allegato contenente un *malaware*. Il problema, una volta in rete, è trovare il punto debole, ovvero la persona o i mezzi giusti da "usare" per ottenere il risultato desiderato.

Nell'esercito israeliano c'è una regola nell'istruzione alla navigazione: se sei

perso e devi tornare, segui la corrente del fiume, alla fine troverai qualcuno. L'hacker segue la corrente del fiume: il personale a partire dagli organi direttivi, che si stanno occupando ad esempio di una fusione o un'acquisizione confidenziale; poi il reparto IT per quanto riguarda documenti, software, server ecc., infine anche terzi esterni. Nell'esempio indicato, se l'intenzione fosse di voler leggere e-mail, l'hacker potrebbe attaccare il computer o il server dove sono custodite (che può essere difficile, visto che qui si trovano concentrati gli sforzi di protezione messi in atto dal reparto IT), o potrebbe anche pensare di attaccare il *backup* dei dati. Inoltre, potrebbe considerare di attaccare anche i sistemi di avvocati e consulenti esterni che si occupano della pratica di fusione e acquisizione, che magari dispongono di un livello di sicurezza inferiore. I temi dell'esternalizzazione (*outsorcing*) di attività e servizi, come pure il *cloud computing* sono, quindi, di estrema attualità e criticità.

L'hacker procede secondo uno schema *OODA loop* (observe, orient, decide, act): questa attività può durare mesi, anche per evitare di essere scoperti. Ben si comprende, quindi, l'asimmetria tra attaccante e attaccato, anche

a livello di tempo di azione rispetto a quello di reazione.

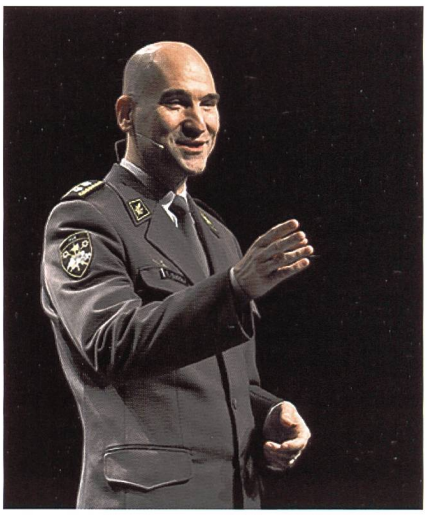
Complessità e tecnologia

Gli strumenti nel tempo sono divenuti sempre più sofisticati e diffusi: anche solo 50 anni fa se un hacker attaccava una banca, a parte la complessità, non aveva la sicurezza che tutto fosse collegato a un sistema informatico accessibile. Di contro, 50 anni dopo tutti sono connessi a internet. E con un elevato livello di connessione si può inserire anche soltanto un dispositivo non sofisticato in rete, ottenendo il medesimo effetto che in passato. Si tratta dell'asimmetria tra connessione e complessità.

Il sistema di difesa di un'azienda o un'istituzione è basato su professionisti IT che agiscono quando vi sono allarmi nel sistema. Saturare il sistema di allarmi può provocare un collasso a causa dei falsi positivi. Vi è, quindi, un'ulteriore asimmetria tra automazione dell'attaccante e automazione del difensore.

Per passare a qualche esempio, un obiettivo classico sono i *point of sale system* (POS) per le carte di credito. Siccome generalmente non possono essere conservate tutte le informazioni sensibili in ogni luogo, l'hacker è spinto a trovare dove può reperire queste informazioni in un solo luogo, come nei POS.

Per quanto riguarda il tema *Know Your Customer*, di rilievo non solo per le banche, interessante per un hacker è l'ambito più generale dell'identificazione delle persone attraverso dati, voce, impronte digitali, viso, password ecc. Ad esempio, l'assistente personale intelligente Amazon Alexa, che consente all'utente di controllare con la voce una molteplicità di oggetti, servizi, contenuti e quant'altro. Per operare un accredito di una somma di denaro con Alexa, devo "delegare" la mia carta di credito e la mia identità ad Alexa. Questa delega a un sistema *proxy* smaterializzato è una sfida non solo per la sicurezza, ma anche per le implicazioni pratiche sull'utente medesimo. Per quanto riguarda il *maschine learning*, non solo nel business, il problema attuale è comprendere per quale motivo un sistema reagisca in un certo modo. Se non si sa perché, un attaccante può vedere un'opportunità, ad esempio nel controllo degli algoritmi sulle immagini. Si può controllare cosa un sistema vede, e *in extremis* si può giungere a modificare in tempo reale, in un video registrato o in una ripresa diretta, il viso di una persona e come si esprime. Già solo con 30 secondi di voce registrata, è possibile modificare la voce di una persone in un filmato.



Israele

Al termine del suo esposto, il relatore ha brevemente illustrato la "dottrina" israeliana, che segue un approccio operativo, i cui punti salienti sono i seguenti:

- raggiungere la superiorità su attori statali nazionali: agire meglio e prima degli altri, senza attendere attacchi;
- sventare/ostacolare attacchi in modo proattivo e più lontano possibile da beni e valori critici per lo Stato;
- cercare di affrontare l'avversario in "un'arena" in cui si è più forti e ci si può difendere meglio;
- selezionare cosa, chi e quali sistemi difendere (difesa differenziata);
- monitorare e comprendere i rischi cyber nello "spettro complessivo", individuando cosa (non) fa il settore pubblico e cosa (non) fa il settore privato;
- selezionare sin dalla giovane età, preparare ed esercitare le persone che si occupano di ciberdifesa;
- esercitare i *decision makers*.

All'incontro ha partecipato anche il divisionario Thomas Süssli, capo della Base d'aiuto alla condotta (BAC) dell'Esercito svizzero, già quadro della banca Vontobel, che ha messo in evidenza gli sforzi e le misure posti in essere dall'esercito per difendersi da eventuali attacchi (v. RMSI 01/2019 pag. 20 e 06/2018 pag. 25 segg.).

Ha evidenziato come il ciberattacco di cui è stata vittima la RUAG (ben 20 Go di dati sottratti!) sia stato il campanello d'allarme a livello Confederazione. Ha deplorato il fatto che molte aziende si sentano al riparo da rischi informatici per il semplice fatto di disporre di un antivirus e poco più. Ha poi citato il rischio di ignorare di essere stati oggetto di attacchi. Il suo consiglio alle banche private è stato di "esercitarsi alle crisi cyber".

Il *Private Banking Day* è stato aperto da Marcel Rohner, presidente dell'Associazione di Banche Svizzere di Gestione Patrimoniale e Istituzionale (ABG) che ha sottolineato come anche per le banche private la capacità di contrastare efficacemente i rischi cibernetici rappresenti un fattore determinante di sviluppo e di successo.

Oltre ai relatori citati, da segnalare l'intervista e la discussione sulle conseguenze per gli attori della piazza finanziaria svizzera, cui hanno partecipato anche Marc Henauer, capo della sezione MELANI del Servizio di informazione della Confederazione, e Ivano Somaini, security analyst e social engineer della Compass Security Schweiz AG, moderati da Katja Stauber.

Yves Mirabaud, presidente dell'Associazione dei banchieri privati svizzeri, nel suo intervento conclusivo, ha auspicato che la Svizzera possa restare, per le banche, un porto attrattivo e sicuro anche in un mondo digitalizzato. ◆