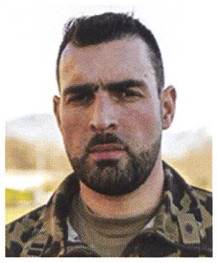
Zeitschrift: Rivista Militare Svizzera di lingua italiana : RMSI
Herausgeber: Associazione Rivista Militare Svizzera di lingua italiana
Band: 90 (2018)
Heft: 1

Rubrik: Circoli, società d'arma e associazioni

Conferenza autunnale 2017 della ATUP sul tema Cyber attacco, dimostrazione pratica



ten col SMG
Gian Domenico Curiale

tenente colonnello SMG
Gian Domenico Curiale

Niente è più disarmante che farsi sorprendere. La storia è ricca di esempi nei quali l'esito di una battaglia è stata decisa, o perlomeno fortemente influenzata, da una novità tecnologica o ideologica. Altrettanto diffuso è il fenomeno di resistenza nei confronti delle novità. L'ATUP ha voluto "prendere il toro per le corna" e sensibilizzare l'ufficialità ticinese sui rischi del fenomeno Cyber svelandone alcuni retroscena. La relatrice, Priska Pietra, si è cimentata in prima persona con la questione presso il NATO Cooperative Cyber Defence Centre of Excellence di Tallinn e ha mostrato in modo pratico, servendosi di un caso fittizio, quali sono i processi propri a un attacco Cyber.
Durante la conferenza è stato dimostrato in che modo delle informazioni apparentemente innocue possano essere usurpate, e sistemi informatici infiltrati, per poter agire in modo inopinato. La *Cyber Kill Chain* utilizzata per pianificare e compiere attacchi informatici è simile al nostro processo di pianificazione. La vulnerabilità dei sistemi informatici e la disponibilità di programmi per sfruttarne le debolezze mettono in evidenza la necessità di proteggere i nostri dati.

Parlare di novità o di sorpresa strategica, riferendosi agli attacchi Cyber, è ormai fuori luogo. Tuttavia nonostante sia sulle labbra di tutti, l'operazione cibernetica non evoca un'immagine unanime. La dipendenza della nostra società dai sistemi informatici non è più un

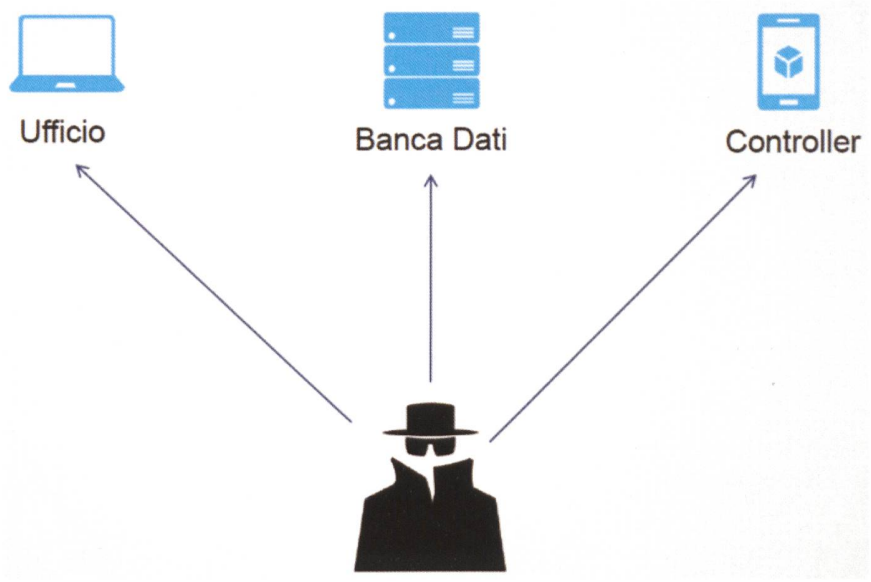
La relatrice, Priska Pietra

segreto. Meno conosciuti sono tuttavia le vulnerabilità dei suddetti sistemi e del ruolo che ogni utente gioca nell'ambito della sicurezza collettiva. Penso, senza voler accusare nessuno, che ognuno di noi abbia trasgredito almeno una volta l'una o l'altra regola di sicurezza informatica. Si voglia per pigrizia, pragmatismo, ignoranza o per non cedere alla Cyber-paranoia. Tali comportamenti, anche se le conseguenze non si manifestano a corto termine, possono tuttavia mettere in pericolo la sicurezza del singolo, dell'azienda o addirittura della collettività. Con abili doti didattiche la giovane neolaureata è riuscita a volgarizzare concetti complessi e dimostrare in modo palese quanto sopra.

La scelta della relatrice **è stata dettata dalla volontà di** approfondire una tematica già introdotta presso gli ufficiali e sottufficiali di professione ticinesi dal Direttore del centro sistemi informativi del Canton Ticino, il col Silvano Petrini. Ogni dirigente è cosciente del fatto che la fattibilità delle sue idee sono tributarie di limitazioni tecniche. Interessandoci alla tecnica e ai processi delle operazioni cibernetiche, volevamo armarci per poter distinguere mito e realtà.

La nostra relatrice, **Priska Pietra** studentessa in informatica al politecnico di Zurigo ha potuto integrare uno dei gruppi di lavoro più avanzati in materia presso il CCDCOE (*Cooperative Cyber Defence Centre of Excellence*) di Tallin. L'Estonia è uno dei paesi più digitalizzati al mondo. Integrando l'alleanza transatlantica nel 2004, l'Estonia propose alla NATO di mettere a disposizione le sue competenze in ambito informatico creando il suddetto centro. Quest'ultimo si

Kill Chain



I punti d'accesso possibili

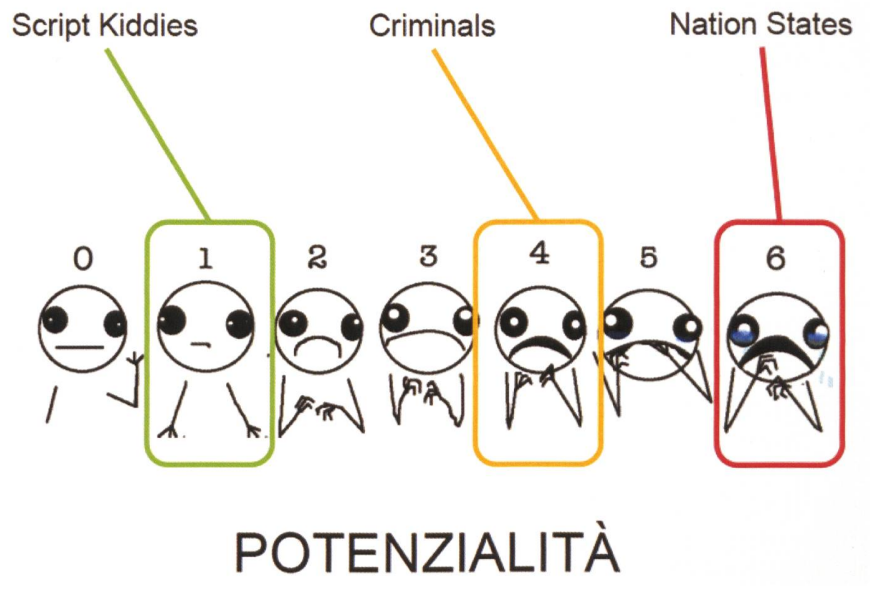
distingue da altri per l'organizzazione di un esercizio di simulazione reale cui il nostro conferenziere ha avuto la possibilità di partecipare nell'ambito dei suoi studi in sicurezza informatica.

Regolarmente i media informano di attacchi informatici, informazioni confidenziali rubate o guasti maggiori a sistemi di aziende e infrastrutture. La concomitanza di un guasto o una fuga di informazioni con una determinata situazione può avere esiti catastrofici. Il nostro processo di condotta militare prevede che, durante la ricerca della decisione di base, analizziamo due aspetti che potrebbero mettere in pericolo la riuscita della nostra missione: le possibilità dell'avversario, e tutta una serie di eventi o di guasti a sistemi, armi e truppa che sono analizzati nell'ambito della gestione dei rischi. Il quesito che sorge spontaneo è di sapere in che misura la disinformazione, il guasto a sistemi o altri ostacoli all'adempimento della missione possano essere opera della controparte.

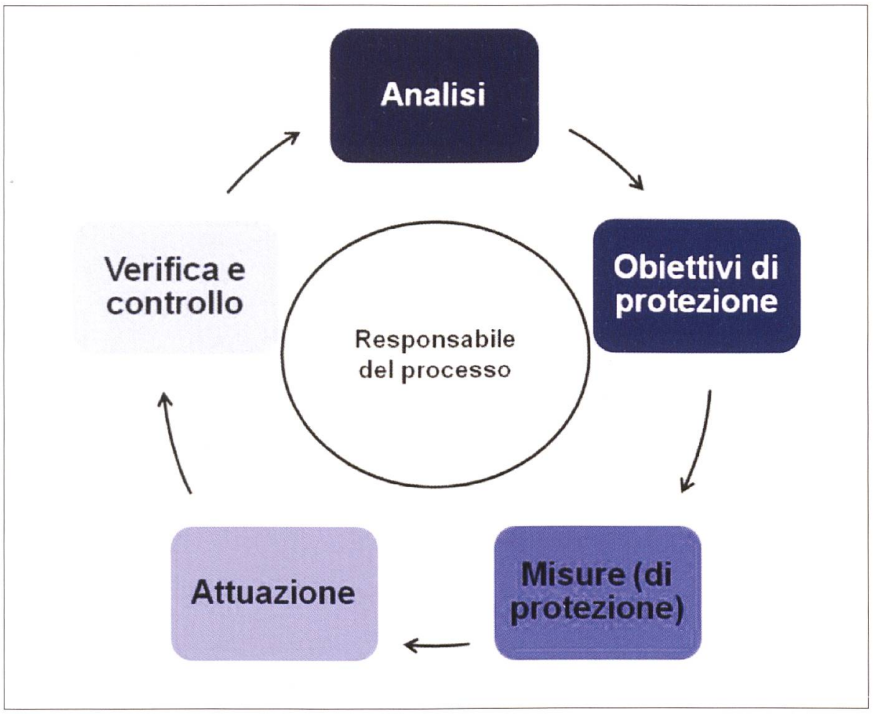
Durante l'esposto sono emersi chiaramente tre insegnamenti principali:

- Il nostro processo di condotta è perfettamente idoneo per analizzare situazioni nel loro insieme. Situazione informatica incluse, a condizione di conoscerne possibilità e limitazioni.
- L'utilizzatore deve costantemente analizzare quali informazioni deve proteggere per evitare che un terzo possa servirsene per recargli un danno.
- I programmi informatici, ormai indispensabili all'onnipresente esigenza di velocità e produttività, sono così complessi e la ricerca è così veloce che l'inviolabilità dei sistemi è utopica.

La *Cyber Kill Chain* è una procedura utilizzata per identificare vulnerabilità da sfruttare, obiettivi e modi operandi di un attacco. Le analogie con il processo di pianificazione in vigore nel nostro esercito sono rassicuranti, ciò mostra che l'approccio è paragonabile a un'operazione detta classica. La novità risiede nel dettaglio dell'analisi. In effetti, per poter provocare la messa fuori servizio di un'istallazione giudicata vitale, è necessario conoscerne i componenti, la versione del programma di gestione e il suo funzionamento. Ciò limita le capacità necessarie per sferrare un attacco spettacolare a criminali e organizzazioni ben informate o ben finanziate. La conoscenza è una prerogativa indispensabile sia al difensore che



Chi è suscettibile di attaccare un sistema informatico?



Come ci si può proteggere

all'attaccante. Il difensore che ignora tali rischi non sente il bisogno di proteggersi in modo adeguato. L'attaccante che, dal canto suo, si priva a priori di un tale mezzo offensivo, rischia di non sfruttare tutte le potenzialità disponibili per raggiungere il suo obiettivo.

La mancanza di conoscenza o l'innocenza smisurata d'oggi giorno fanno sì che sottovalutiamo il rischio rilevando o proteggendo male informazioni apparentemente innocue. In una società altamente automatizzata e connessa, il "tallone d'Achille" resta e resterà l'uomo! Per danneggiare modificare i parametri di una macchina o di un computer bisogna accederci fisicamente o via una connessione internet. La seconda variante è favorita dall'aggressore poiché più discreta. Essa permette di camuffare l'intrusione e restare attivo per più tempo. L'utente, a cavallo tra protezione della privacy e necessità di rendersi visibile in rete, pubblica spesso informazioni preziose. L'aggressore cibernetico, grazie alle ormai inevitabili tracce che lasciamo giornalmente in rete, riesce a interconnettere informazioni e dati per identificare possibili punti d'accesso. Quando riceviamo e-mail o link da fonti e/o con soggetti coerenti con le nostre attività in rete, rischiamo di aprire la porta all'aggressore senza rendersene conto. Meno tracce lasciamo, più è difficile per l'aggressore identificare chi lavora con chi e a quali informazioni ha accesso.

A priori il "ridotto cibernetico" può sembrare la soluzione, ma disconnettersi e isolarsi vuol dire rinunciare anche ai continui aggiornamenti dei nostri programmi. La corsa contro il tempo per correggere le lacune al sistema di sicurezza crea anche tutta una serie di prodotti secondari. Applicazioni e soluzioni per sfruttare le lacune menzionate sono facilmente disponibili sulla rete. Neanche in informatica la protezione garanzia al 100% non esiste. Distinguere buoni dai cattivi è una lotta vecchia come il mondo. Tenersi aggiornato, esser prudente e aver un pizzico di fortuna rimane ieri come oggi l'unica soluzione.

Se la nostra conferenza è riuscita a sensibilizzare il pubblico presente, allora abbiamo contribuito a salvaguardare un po' di sicurezza collettiva. Il concetto di sicurezza non riposa unicamente sulla difesa ma è un concetto globale e interministeriale. Per dare continuità al concetto di sensibilizzazione alla sicurezza abbiamo invitato per la prossima conferenza il signor **Samuel Bontadelli**, membro Direttore e COO (Responsabile operativo) del Gruppo Repower, per capire quale ruolo l'approvvigionamento energetico gioca nella sicurezza e nella stabilità del nostro Paese.

Ringraziando nuovamente la relatrice Priska Pietra per la sua disponibilità e felicitarla per la brillante prestazione, dò appuntamento a quest'autunno per la conferenza sopracitata. ◆

Ten col SMG Gian Domenico Curiale – Ufficiale di carriera, brevettato alla 22° promozione della Scuola di Guerra di Parigi, ha servito quale istruttore principalmente presso le scuole reclute di fanteria, dall'istruttore d'unità sino a comandante del battaglione di fanteria di ferma continua 142, e presso l'istruzione superiore dei quadri dell'esercito, dallo stage di formazione per futuri ufficiali sino al corso di formazione alla condotta II. Quale ufficiale di milizia ha servito in diverse funzioni, nell'ambito dell'aiuto alla condotta presso lo stato maggiore di brigata di fanteria di montagna 9 sino a occupare la funzione di sottocapo di stato maggiore aiuto alla condotta. In questo momento è professionalmente impiegato quale responsabile per l'istruzione di base in seno al corso di formazione per corpi di truppa e, in veste di ufficiale di milizia, serve quale sottocapo di stato maggiore territoriale (G5) presso la divisione territoriale 3.

Priska PIETRA – Master in informatica presso il politecnico di Zurigo, ha frequentato uno stage presso il NATO Cooperative Cyber Defence Centre of Excellence di Tallinn in ambito della sicurezza informatica. Attualmente è impiegata presso la Base d'aiuto alla condotta dell'esercito.

Voi contate sulla disponibilità. Noi forniamo soluzioni affidabili.

RUAG Aviation è il vostro partner affidabile nella gestione fornita ad aerei, elicotteri e sistemi lungo il loro intero ciclo di vita. Manutenzione tecnica, modifiche, upgrade o integrazione di sistemi: i nostri specialisti vantano un ampio know how e un bagaglio di esperienza pluriennale. Con i nostri servizi garantiamo una durata dei vostri sistemi superiore alla media e tempi di turn-around più brevi consentono un impiego più rapido: un valore aggiunto molto apprezzato dai nostri clienti nel campo militare e civile in tutto il mondo.

RUAG Schweiz AG | **RUAG Aviation**
Casella postale | Aerodromo | 6527 Lodrino | Svizzera | Tel. +41 91 873 41 11
info.lodrino.aviation@ruag.com | **propeller-aircraft.ruag.com**

Together ahead. RUAG