Battaglie cruenti, ma senza spargimento di sangue

Autor(en): **Bögli, Thomas**

Objekttyp: **Article**

Zeitschrift: **Rivista Militare Svizzera di lingua italiana : RMSI**

Band (Jahr): **92 (2020)**

Heft 5

PDF erstellt am: **28.06.2024**

Persistenter Link: https://doi.org/10.5169/seals-913821

Battaglie cruenti, ma senza spargimento di sangue

Phishing, software dannosi (malware), ransomware e virus di ogni genere: attualmente i ciberattacchi sono di varia natura e spesso difficili da individuare. Nessuno ne è al riparo: né il singolo individuo, né le grandi imprese e nemmeno le pubbliche amministrazioni.

Comunicazione Difesa

Per prevenire meglio queste minacce, il Consiglio federale ha approvato la creazione di un centro di competenza contro i ciberrischi. È l'occasione per fare il punto della situazione con Thomas Bögli, specialista e capo Cyberdefense dell'Esercito svizzero.

Signor Bögli, com'è organizzata la ciberdifesa in Svizzera?
In Svizzera la regola d'impiego definisce che ciascuno è responsabile della propria sicurezza. Le infrastrutture critiche, vale a dire le imprese come ad esempio la Posta, Swisscom, le banche ecc. sono responsabili della propria sicurezza. A livello federale la Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI), diretta congiuntamente dal Dipartimento federale delle finanze (DFF) e dal Dipartimento federale della difesa, della protezione della popolazione e dello sport (DDPS), riveste un ruolo centrale. Si prefigge di prevenire e gestire i ciber-rischi e fornisce il proprio sostegno alle infrastrutture critiche. Parallelamente, la lotta contro la cibercriminalità spetta al Dipartimento federale di giustizia e polizia (DFGP) che possiede un Servizio di coordinazione per la lotta contro la criminalità su Internet (SCOCI).
Per chiarire e centralizzare questa organizzazione, il Consiglio federale ha approvato la creazione di un centro di competenza in materia di cibersicurezza. Questo centro è guidato da un delegato alla cibersicurezza e funge da primo punto di contatto per tutte le questioni relative ai ciberrischi.

Thomas Bögli, capo Cyberdefense dell'Esercito svizzero. ©VBS/DDPS – Comca D

Qual è il ruolo dell'esercito nella ciberdifesa?
Come per le infrastrutture critiche, l'esercito deve innanzitutto garantire la propria protezione. Ciononostante può essere chiamato a fornire un appoggio sussidiario alle autorità civili in caso di ciberattacco di vasta portata. La missione "aiutare, proteggere, combattere" è valida anche nel ciberspazio.

Con quale frequenza la Svizzera è vittima di ciberattacchi?
Quotidianamente! Ogni giorno si verificano tentativi di ciberattacco in Svizzera. Spesso le imprese interessate non se ne rendono nemmeno conto, oppure non rivelano niente per paura di compromettere la propria reputazione. I ransomware, ad esempio, sono all'ordine del giorno. Si tratta di software che cifrano i dati di un singolo individuo o di un'impresa rendendoli inaccessibili. Gli hacker chiedono quindi un riscatto in cambio della chiave per decifrare questi dati.

Chi si cela dietro questi attacchi?
Esiste una piramide con cinque differenti tipi di aggressori. In cima troviamo le ciberpotenze, come la Cina, la Russia, gli Stati Uniti, la Gran Bretagna o Israele. Si tratta di una guerra senza armi letali, senza spargimento di sangue e senza morti, ma il cui obiettivo è il furto di dati. Nel 2016, ad esempio, la RUAG è stata vittima di ciberspionaggio ed è stata derubata di dati importanti.

In che modo può proteggersi l'esercito?
La competenza per la ciberdifesa dell'esercito spetta alla Base d'aiuto alla condotta (BAC). Abbiamo bisogno di validi rilevatori di malware e collaboratori attenti all'evoluzione della situazione nel ciberspazio. In fin dei conti, quando sopraggiunge un ciberattacco l'esercito deve essere in grado di accerchiarlo e isolarlo rapidamente.

Rispetto ad altri paesi, qual è il livello di preparazione della Svizzera?
Qualitativamente abbiamo un buon livello di preparazione. Quantitativamente invece disponiamo di poche risorse a livello di personale. Fortunatamente le scuole reclute in ambito cyber permetteranno di fornire un apprezzato supporto ai ciberspecialisti di professione della BAC. Qualora l'esercito dovesse appoggiare le autorità civili, questi militari della milizia garantiranno un impegno sul lungo periodo.

La guerra del futuro si farà soltanto a colpi di computer?
Non penso che il "cyber" sostituirà i mezzi esistenti. Nel 1914, ad esempio, l'introduzione delle forze aeree non ha rimpiazzato le truppe al suolo. Alla stessa stregua l'ambito cyber è una dimensione supplementare che va ad aggiungersi alle dimensioni terrestre e aerea. In un certo senso l'esercito è come un coltellino svizzero e il cyber è una componente in più che deve essere integrata.

Quale capo Cyberdefense dell'esercito, quali sono le principali sfide dei prossimi anni?
In primo luogo l'Internet delle cose (*Internet of Things*, IoT), ossia tutti gli apparecchi connessi, dalle automobili alle televisioni, fino ai frigoriferi. Questi apparecchi rappresenteranno una fonte di pericolo in quanto i sistemi di difesa sono troppo deboli. Abbiamo a che fare con la questione della sicurezza nel suo complesso e del trattamento dei dati registrati da questi oggetti. Cosa ne facciamo di questi dati? Come facciamo ad essere sicuri che non saranno utilizzati in modo improprio?
Per quanto riguarda l'esercito in particolare, si tratterà di sapere cosa ci si attende da parte sua in caso di ciberattacco. Occorrerà definire chiaramente e quantificare l'appoggio sussidiario che l'esercito potrà essere chiamato a fornire alle autorità civili.

Quali consigli di base darebbe alla popolazione affinché si protegga dai ciberattacchi?
Dico sempre che bisogna essere "paranoici in modo costruttivo". Scherzi a parte, esistono alcune semplici regole da seguire. Bisogna diffidare dai Wifi gratuiti e disattivare il WLAN o il Bluetooth se non ne avete bisogno. In caso di colloqui confidenziali si consiglia di metter via smartphone e altri potenziali apparecchi spia. Senza sconfinare nell'isteria, bisogna sempre essere prudenti. E se riscontrate un problema, prendete immediatamente contatto con la Centrale MELANI. ◆