Cybersecurity: cyberattacchi negli Enti ecclesiastici. Scenari, difese e mitigazione del rischio

di ***Christian Buangjug***

L'evoluzione dell'informatica ha posto la tecnologia al centro della riflessione sui nuovi costumi delle generazioni attuali e future. Siamo a un *turning point* in cui si cominciano a produrre chip quantistici in grado di competere con i supercomputer tradizionali (che producono miliardi di miliardi di processi al secondo; e tale cifra è da interpretarsi alla lettera) e l'IA, l'intelligenza artificiale, sta prendendo la forma che sempre ha abitato l'inconscio collettivo tramite la finzione letteraria o cinematografica.

Gli attuali supercomputer provengono in gran parte dal sistema pubblico e impiegano l'equivalente in anni del numero dieci seguito da venticinque zeri per fare quello che un chip quantistico risolve in pochi minuti.

Questo, chiaramente, evidenzia delle criticità sulla sicurezza dei sistemi. Un chip quantistico è virtualmente in grado di bucare qualsiasi sistema in un tempo brevissimo; ed è per tale motivo che la crittografia che si

sta sviluppando in ambito accademico è una crittografia *ad hoc* per questa casistica contemporanea.

Più volte sono apparse sui quotidiani nazionali notizie riguardanti attacchi hacker da parte di attori internazionali (**APT**, *Advanced Persistent Threats*, come il gruppo nordcoreano Lazarus) ai danni di istituzioni pubbliche, infrastrutture, portali della pubblica amministrazione. La verità è che, benché alcuni attacchi si siano effettivamente realizzati tramite strategie complesse, gli attacchi più efficaci sono risultati quelli che hanno maggiormente sfruttato la mancanza di una cultura della protezione dei propri dispositivi, ovvero il persistere del dubbio e dell'errore in soggetti non tecnicamente formati, collocati in posizioni critiche per la tenuta della struttura informatica.

Quali sono gli attacchi più comuni, con quale frequenza avvengono e quali sono i cybercriminali e le loro intenzioni? Il presente articolo illustra alcune pratiche che possano portare i lettori a una maggiore attenzione nelle proprie abitudini e a comprendere che, nell'informatica, se una cosa può teoricamente essere realizzata, vi è un'elevata probabilità che qualcuno la realizzi. Perciò è importante fare controlli ciclici nelle proprie reti e nei propri dispositivi (nominando, possibilmente, un responsabile), dal momento che un hacker malintenzionato può rimanere nascosto in un sistema per anni. Se non viene tracciato, virtualmente può esserlo per sempre.

Il mondo AGIDAE abbraccia fondamentalmente attraverso i CCNL tre settori di attività: la scuola, il settore sociosanitario-assistenziale e le università pontificie. Ciascuno di questi settori ha delle proprie criticità.

Il settore scuola ha interesse ad avere una politica di difesa dei propri dati (perciò anche di *storage*, ovvero di allocazione dei dati, che può essere inteso in termini fisici), ma chiaramente nell'ipotesi in cui i computer degli uffici amministrativi venissero infettati da un *malware* (quello che anni fa veniva chiamato un virus) da quei computer potrebbero essere esfiltrate credenziali che appartengono a tutte le strutture collegate dell'Ente giuridico, della congregazione, dei superiori di ogni ordine e grado o delle comunità presenti in altri continenti. Di qui la necessità di estendere le politiche di difesa anche verso questi altre aree geografiche nel caso in cui si riscontrasse in loco una reale carenza di figure professionali adeguate.

Analoghe considerazioni potrebbero farsi per una struttura ospedaliera. Tutto ciò che è software può essere piegato alla volontà di un programmatore esperto. Un hacker può non solo rubare un database o comprometterlo, ma può anche mettere in disordine i dati registrati, creando confusione nelle cartelle cliniche e nella archiviazione diagnostica. In via del tutto teorica (tuttavia una possibilità non così remota) un hacker può installare un malware nel telefono di un paziente ricoverato, il quale, connessosi alla rete wireless, può installare altro malware nella rete interna, infettando altri pazienti e, virtualmente, anche macchinari che non sono in ambiente *sandbox*, ovvero protetto.

Il settore *Università* può risentire di attacchi dimostrativi (come un *defacciamento*, che si ha quando la prima pagina del sito dell'ateneo viene sostituita con un messaggio politico, sociale, di protesta o di semplice vandalismo) oppure possono essere manomessi i libretti degli studenti, creando un problema nello storico della carriera accademica di ciascuno dei discenti, ormai reso inattendibile. Lo stesso può accadere per tutta la documentazione accademica relativa anche ai profili professionali del personale docente, non docente e dirigente.

È bene, quindi, conoscere i responsabili di questi esperimenti più o meno irrimediabili. C'è da dire che la cultura hacker ha subito una evoluzione, che è andata di pari passo sia con lo sviluppo di nuovi linguaggi di programmazione e di tecnologie (come le reti neurali artificiali), sia con il progressivo evolversi di Internet in favore di una maggiore tutela dei dati, a livello *corporate* e a livello normativo. Per fare un esempio, fino a circa dieci anni fa era possibile scaricare software piratato per Windows e Mac; chiunque provi a fare ora lo stesso, tranne alcuni rari casi da valutare comunque con attenzione, probabilmente installerebbe sul proprio sistema un malware, ovvero un software malevolo. E chiaramente, dovendo usare la password di amministratore per installare il software illegale, darebbe al malware la possibilità di avere il controllo sulla propria macchina.

Ma gli hacker, sia di buoni, sia di cattivi principi etici (gli hacker etici sono detti tali solo perché si mantengono entro i limiti della legalità; ma uno stesso hacker etico per la propria nazione può essere un pericolo per una nazione avversaria, come la storia recente della *cyberwarfare* internazionale ha dimostrato; si tratta generalmente di persone che sperimentano con il codice e che hanno una grande immaginazione astratta nella creazione di algoritmi che vadano a colpire obiettivi della realtà, sia su dispositivi propri, sia su macchine distanti connesse in rete.

Moltissimi hacker, tuttavia, non hanno grande esperienza di programmazione e usano dei software disponibili gratuitamente per l'hacking etico, i quali, pur gratuiti, sono strumenti molto potenti. Questi hacker vengono chiamati ironicamente *script kiddies*, ovvero "ragazzini da script", ma non per questo sono meno pericolosi. Sono anzi molto ossessivi e meticolosi, e attaccano obiettivi abbordabili in quantità massicce, spesso in modalità automatizzata, violando sistemi perfino nel sonno, mentre il loro computer è attivo. Per fare un esempio, il software *massscan* (scansione di massa) è in grado di scannerizzare le porte di tutta Internet in 4 minuti e mezzo. Oppure **metasploit** è un software che esce di default carico di una quantità sorprendente di **payload**, ovvero di attacchi e malware, sia per i telefoni, sia per Windows e Linux, mentre il software **hydra** può provare tutte le password del file **rockyou.txt** (un database esfiltrato con 14 milioni di password non criptate) in circa 3 giorni su una casella e-mail. *Repetita iuvant*: questi programmi sono gratuiti e vengono eseguiti da terminale *Linux*, ovvero tutto in maniera gratuita ed accessibile.

Quali sono gli obiettivi sensibili e per quali motivi vengono attaccati?

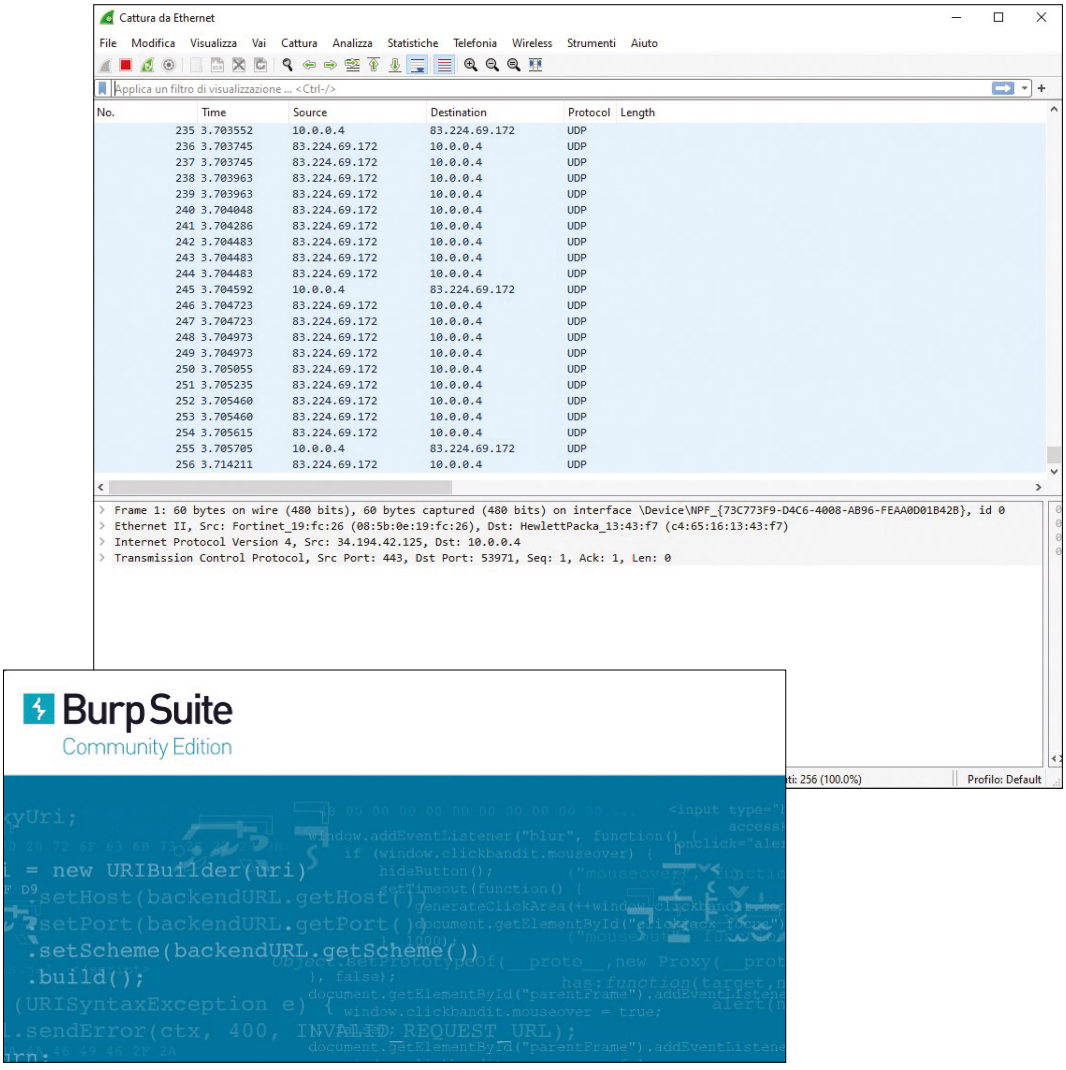
Il mondo di Internet ha mostrato più volte le mille sfaccettature della psicologia dei suoi utenti. Il dark web, così come il deep web, offre migliaia di servizi che servono a compiacere deviazioni perverse, così come bizzarri modi goliardici di adunarsi di fronte a un contenuto multimediale. L'estetica e la psicologia di questi fenomeni non sono mai state definite in termini generali. Chiaramente, questi eventi possono avere luogo in seguito a una transazione (solitamente in Bitcoin) oppure gratuitamente, se lo scambio di file e link avviene su un server del deep web, come un server privato il cui link è conosciuto solo dagli interessati. I link del dark web sono impossibili da "indovinare" o indicizzare. Ecco, per fare un esempio, il link per il dark web del New York Times, usato per le rivelazioni delle gole profonde o il whistleblowing:
https://www.nytimesn7cgmftshazwhfgzm37qxb44r64ytbb2dj3x62d2lljsciiyd.onion/

Se non fosse stato per il protocollo TOR, usato per connettersi al dark web, e per il sistema operativo *Linux Tails*, Edward Snowden non avrebbe mai potuto contattare i giornalisti che hanno divulgato le sue rivelazioni sulla NSA.

Sul dark web possono essere **vendute, ad esempio,** informazioni riguardanti enti e strutture del mondo ecclesiastico: **credenziali social, e-mail e SPID, dump di database, "remote access" per inserire i dispositivi su una botnet, link in diretta da telecamere private, estremi delle carte di credito, documenti per falsificazione, dati biometrici e tutto ciò che può essere esportato da un dispositivo.**

Da dove entrano, pertanto, i cosiddetti hacker? Quali sono le vulnerabilità che permettono loro di penetrare nei sistemi? A seguire saranno spiegati i termini tecnici sopra citati.

Ogni dispositivo connesso a Internet può essere visto da qualsiasi altro dispositivo utilizzando gli opportuni strumenti. Sono



perciò vulnerabili i singoli PC o Mac, i server, i dispositivi IoT (Internet of Things, che comprende dispositivi come il frigorifero smart o l'aspirapolvere smart) gli smartphone, le telecamere e qualsiasi device sia connesso e controllabile via rete.

Un particolare tipo di hacker, noto come **bot herder** (ovvero "pastore di bot", diminutivo di "robot") può hackerare un pc per il semplice scopo di mantenere l'anonimato. Questi hacker vengono chiamati "pastori" perché possono arrivare ad hackerare decine di migliaia di computer, il tutto senza rendere evidente alcuna attività anomala e aumentare il livello di allarme. Sono infatti tali reti, di cui essi sono padroni nascosti, a essere chiamate **botnet**, che significa "rete di robot". Rintracciare un bot herder è molto difficile, ma non impossibile. Può ad esempio rendersi scoperto in una transazione in cui l'herder vende parte della sua rete ad altri hacker per lanciare attacchi decentralizzati.

Cosa invece si intende per "dump di database"? Semplicemente è una copia intera,

oppure una replica, di un database di un server. Una volta hackerato un server, un hacker può copiare il database su un suo server proprio e venderlo sul dark web. Il più delle volte ciò avviene in concomitanza di un attacco ransomware (ransom significa "riscatto"), dove i file di un database vengono criptati e resi inutilizzabili. Alla richiesta di una chiave che sblocchi i file criptati si chiede un riscatto in Bitcoin o in altre criptovalute come Monero (considerato sul dark web l'unica valuta veramente irrintracciabile, al contrario di Bitcoin ed Ethereum). Se il riscatto non viene pagato, il database viene reso pubblico o venduto sul dark web.

Perciò *è importante rendersi conto che la compromissione di un dispositivo singolo, come un PC o uno smartphone, può compromettere l'intera rete e perfino gli interi server*. Esistono delle precauzioni e degli accorgimenti per rendersi conto se si è stati violati. Ecco due modi per rendersi conto di violazioni dei propri dispositivi:

1) un'analisi delle porte del firewall può evidenziare delle porte aperte molto sospette, note come **backdoor**. Le porte di un firewall sono numerate da 1 a 65565, ma solitamente a ogni protocollo corrisponde una porta specifica e con un valore basso. Il fatto che una porta con un numero insolitamente elevato sia aperta e per servizi già disponibili sulle loro porte standard, rende evidente una falla da cui un hacker può entrare o permettere l'accesso ad altri. E' importante fare questi controlli ciclicamente
2) fare **un'analisi dei pacchetti con Wireshark** in uscita da un dispositivo ci permette di capire il contenuto effettivo del traffico in uscita dei nostri dispositivi. È anche possibile rendersi conto se le credenziali inviate sono crittografate o in chiaro, ma in particolar modo, se si dovesse notare un'attività insolita, come ad esempio qualche strano link, è importante intervenire e cercare le cause o i software (solitamente software piratati o freeware) da cui esce questo traffico di dati.

Quali sono le risorse di cybersecurity utili agli enti o per chi ne cura la parte informatica?

Esistono fondamentalmente tre tipologie di risorse utili per gli enti gestori in materia di cybersecurity:

1) siti web che permettono di scoprire **se i nostri dati sono stati hackerati** o pubblicati sul dark web;
2) database privati o governativi che permettono di comprendere **se le nostre tecnologie sono all'altezza** degli standard di sicurezza;
3) siti di **notizie di cybersecurity** aggiornati ogni settimana.

Nella prima categoria rientra un sito celeberrimo chiamato **"HaveIBeenPwned"** (haveibeenpwned.com), che significa "sono stato hackerato?" e che fa delle ricerche su internet per capire se tra i database che sono stati esfiltrati compare la nostra mail. Un sito simile è **pentester.com** dell'hacker etico Ryan Montgomery (recordman delle CTF, ovvero le competizioni di cybersecurity), che cerca sul dark web il nostro sito web o la nostra mail per vedere se sono state pubblicate le nostre credenziali.

Nella seconda categoria rientra un sito che ha un ruolo centrale nella sicurezza tecnologica delle aziende, che appartiene al NIST (National Institute of Standard and Technology). Il sito a cui ci riferiamo è il **National Vulnerability Database** (nvd.nist.gov), dove sono raccolte tutte le tecnologie che sono state craccate e che sarebbe bene non comprendere nelle proprie strutture.

Oltre ad esso c'è il famoso **Shodan** (shodan.io), che è stato definito *"il Google degli hacker"*, perché su questa piattaforma sono raccolti tutti i dispositivi collegati a Internet del mondo. È possibile da qui vedere le telecamere che non sono protette da password (per cui dovreste **sempre** scegliere una password diversa da quella di fabbrica per le vostre telecamere, dal momento che esistono **database pubblici** con le password di default per ogni dispositivo, catalogate per marca e modello del prodotto) o anche impianti industriali, server, dispositivi IoT. Chiunque possieda dei computer con versioni obsolete di Windows, come Windows XP o Windows 7, è bene che sappia che su **Shodan** è possibile risalire a queste macchine, con esposti l'indirizzo IP e la posizione geografica, con associato il rischio che l'intera rete a cui sono connesse venga compromessa. Un altro esempio è **MITRE ATT&CK**, un sito web della MITRE Corporation dove sono raccolte tutte le procedure di attacco e di difesa nel mondo cyber. In esso sono inclusi gli **attacchi mobile**. Insieme a **CISCO TALOS**, è uno dei maggiori servizi di **threat intelligence**, che aiuta a realizzare un'analisi delle vulnerabilità dei dispositivi.
Infine ci sono i siti di notizie tra cui **Krebs On Security** (che commenta notizie importantissime sulla cybersecurity, in particolare sugli attacchi hacker degli APT o sui forum di cybercriminali sul dark web) e **The Hacker News**. È sufficiente leggere questi siti web settimanalmente per avere un aggiornamento costante per le proprie macchine.

Come è possibile testare oggettivamente la sicurezza della rete degli istituti o dei loro metodi di difesa?

La premessa fondamentale è che si installino **tutti gli aggiornamenti** e che vi siano le versioni più aggiornate di tutti i software (anche sui dispositivi mobile). In secondo luogo è bene dotarsi di un firewall e di un IDS (Intrusion Detection System) e un IPS (Intrusion Prevention System) e in ultimo è possibile inserire nella propria rete un **honeypot**, ovvero un server facile da hackerare, con informazioni false e che però raccolga informazioni utili per rintracciare chiunque sia in grado di violarne i sistemi di sicurezza.
Ciò premesso, è consigliabile affidarsi agli esperti e alle aziende di cybersecurity, in primo luogo per fare un ***penetration testing***, ovvero un test di penetrazione, al quale segue un rapporto dettagliato con tutte le vulnerabilità e le criticità.
Per condurre un penetration testing bisogna discutere in primo luogo le *rules of engagement*, ovvero le regole d'ingaggio, per evitare, ad esempio, che i database vengano modificati, oppure che si hackeri persone nel consiglio direttivo o anche, in termini tecnici, che si possano hackerare macchine esclusivamente nell'intervallo 10.10.100.101-255.
Se già si dispone di un team di cybersecurity è possibile attuare il cosidetto ***blue teaming-red teaming***, dove la squadra "blu" di difesa deve evitare che venga hackerata la rete dall'azienda "rossa" che conduce il penetration testing.
È inoltre consigliabile applicare tutte le pratiche di *hardening* dei sistemi operativi di tutti i dispositivi e della rete, ovvero di **rafforzamento e prevenzione** nel caso di attacchi reali.
Per concludere: è utile mantenersi aggiornati sui siti sopra indicati perché in questo periodo storico anche la cybersecurity sta seguendo l'evoluzione delle intelligenze artificiali, e perciò, benché anche le difese ne risultino avvantaggiate, i cyberattacchi possono diventare molto più numerosi, frequenti, pericolosi.