FOCUS/ LA RIVOLUZIONE DEL 5G

I buoni in guerra contro i cattivi della rete «Aziende e cittadini, siamo tutti a rischio»

Gianluca Dini, direttore del master in cyber security: come malware, phishing e denial of service si insinuano nel nostro pc

Danilo Fastelli

Occhio alle chiavette usb e alla gestione delle password. La sicurezza informatica in azienda passa anche dalle precauzioni che ogni dipendente può prendere. Ma ancora di più dalla consapevolezza dei rischi da parte dei vertici. «La cyber security deve entrare in consiglio di amministrazione» è il mantra di Gianluca Dini, docente di ingegneria informatica dell'Università di Pisa e direttore del master di primo livello in cyber security – il primo del genere in Toscana – realizzato dall'ateneo pisano in collaborazione con il Cnr.

Se fossimo in un film della Marvel saremmo alla futuribile accademia del professor Xavier, mentore e formatore degli X-Men. Nella saga di Harry Potter ci troveremmo negli scantinati del castello di Hogwarts a lezione dal professor Piton, grande esperto di «difesa contro le arti oscure». Insomma, qui a Pisa si formano i "buoni" che devono proteggerci contro i superpoteri dei malintenzionati della rete. Le allusioni al cinema fantasy sono scontate tra questi banchi frequentati perlopiù da neolaureati in informatica e nerd affini. Ma tra gli allievi del master (in questi giorni si chiude la seconda edizione e comincia la terza, mentre c'è già chi chiede infomazioni per candidarsi alla quarta) ci sono stati anche filofosi, avvocati e professionisti in carriera che hanno fiutato il vento e visto la possibilità di riqualificarsi per migliorare la propria posizione in azienda o cambiare mestiere: le lezioni si concentrano tra il venerdì pomeriggio e il sabato proprio per andare incontro agli studenti-lavoratori.

«Non prendiamo tutti – precisa Dini – perché il master ha un taglio fortemente ingegneristico, quindi o uno ha una laurea specifica o ha un background professionale che consente di padroneggiare le basi». Il master è nato proprio per rispondere alla crescente domanda delle aziende di esperti in sicurezza. «Per comprendere il bisogno basta sfogliare i giornali, le pagine di cronaca e degli annunci di lavoro. I sistemi informatici stanno diventando sempre più pervasivi in tutti gli aspetti della società. Tutto ciò che è in rete ed è informatico è un possibile bersaglio. La cyber security è diventata dunque irrinunciabile per aziende e pubbliche amministrazioni».

La lezione del professor Gianluca Dini comincia con l'analisi delle minacce. «Il lavoro di chi si occupa di sicurezza è ingrato. Il nostro avversario deve trovare un solo punto debole per colpirci; noi invece dobbiamo trovarli tutti e rinforzarli. È uno scontro un po'impari anche perché noi, a differenza dei nostri avversari, dobbiamo rispettare la legge» . «Tra gli attacchi tipici – spiega – ci sono i malware, che vengono prodotti a cadenza giornaliera; gli attacchi via web, il phishing e il denial of service».

A minacciarci possono essere i soggetti più disparati e per le motivazioni più diverse. «I soldi sono in genere il motore principale.

Personalmente mi sono occupato di casi abbastanza emblematici. Per esempio in una grande assicurazione con un sistema tecnologico all'avanguardia ci fu una truffa da parte di un dipendente infedele che utilizzava le password dei colleghi. A dimostrazione che la sicurezza non passa solo dalla tecnologia ma anche banalmente dalla gestione aziendale». Non ci sono solo i soldi, ovviamente. «In un altro caso il dipendente di un'azienda simulava delle truffe per mettere in cattiva luce un collega che era un suo rivale in amore. Insomma anche qui valgono tutte le motivazioni che portano a delinquere nella vita normale».

I soldi, il potere, l'ideologia ma anche la politica. Spesso gli attacchi sono condotti dagli Stati stessi, come nel caso del famigerato malware Stuxnet per bloccare, a partire dal 2006, lo sviluppo del programma nucleare iraniano. E di geopolitica della sicurezza informatica si torna a parlare in questi giorni. Ad allarmare sono gli interessi delle multinazionali cinesi nella costruzione delle reti 5G in Occidente. Dopo gli Stati Uniti, anche l'europarlamento ha messo sull'avviso i Paesi, mentre l'Italia si è affrettata a togliere il fascicolo 5G dal prossimo possibile accordo sulla Via della Seta. «Il tema – spiega Dini – è di estrema delicatezza. Astrarrei dal caso specifico per dire che se c'è una tecnologia che mette in collegamento la pubblica amministrazione, la difesa, i servizi essenziali, sarebbe meglio averne il pieno controllo. Se invece la compro da altri faccio un atto di fede sul fatto che non nasconda trucchi e "backdoor" che permettano a chi me la vende di interferire o controllarmi in futuro».

Per la stessa ragione lo smartphone del ministro della Difesa o dell'ad di una multinazionale non è acquistato al negozio di elettronica dietro l'angolo: è concepito appositamente per rispondere ad esigenze di sicurezza particolari. Ma sbaglia chi pensa che a difendersi debbano essere solo gli obietti più vistosi. «Tutti coloro che fanno uso di sistemi informatici sono a rischio. È chiaro che per una piccola azienda è più complicato perché ha un budget limitato. Perciò con la Regione Toscana stiamo pensando a un progetto che permetta alle piccole imprese di mettere a comune alcune risorse, per esempio conservare i dati su un cloud gestito professionalmente».

I dati personali dei clienti sono il bersaglio più appetibile: numeri di carte di credito ma anche semplici nomi e cognomi, come nel caso – era il 2015 – degli illustri frequentatori del sito di incontri extraconiugali Hashley Madison: molti vennero ricattati, qualcuno arrivò al suicidio. Ma si può prendere di mira anche il sistema produttivo di un'azienda. «Mettiamo che ci sia un mio concorrente che fa meccanica di precisione. Io entro nel suo processo produttivo e altero leggermente la configurazione di un robot, facendogli fare un errore di un micron. Lui pensa di mettere sul mercato viti ad alta precisione che invece sono sbagliate. Così facendo posso provocargli un danno economico enorme».

Per i ricercatori è una corsa contro il tempo perché gli oggetti in rete si moltiplicano e diventano anche sempre più personali: dalle automobili intelligenti (per non parlare di quelle che si guidano da sole), agli smartwatch (in teoria dai movimenti del polso si può ricostruire il codice pin di una carta di credito), ai pacemaker (nel 2013 l'ex vicepresidente Usa Dick Cheney fece disabilitare dal suo la possibilità di configurarlo senza doverlo estrarre chirurgicamente), alle pompe di insulina e persino, ebbene sì, ai sex toys, almeno quelli controllabili in remoto da parte del partner.

Insomma, come Dini ama ripetere, «la pericolosità degli attacchi è limitata soltanto dalla fantasia di chi li mette in pratica». Sebbene per un attacco sofisticato serva la collaborazione «tra più persone molto competenti, con una forte motivazione ideologica o economica».

Da un certo livello in poi, il gioco si fa duro e richiede molte risorse. «E l'Italia può contare su competenze eccezionali nei suoi settori strategici» . —

LE MINACCE TIPICHE

Malware, software malevolo che induce l'utente a installarlo sul proprio sistema. Ne vengono prodotti a cadenza giornaliera. A produrli possono essere amatori come team finanziati addirittura dagli Stati.

Attacchi dal web: tutto ciò che informatico è un programma. E il programma contiene degli errori. Molti di questi errori possono essere sfruttati per mettere in atto degli attacchi.

Attacco phishing. Qui l'anello debole della catena di sicurezza è proprio l'umano. Arriva una mail che pubblicizza un'offerta imperdibile, si apre e quest'azione scatena l'installazione di un malware.

Attacchi "denial of service" (negazione di servizio): un sistema viene sovraccaricato in modo tale da non permettergli più di lavorare.

GIANLUCA DINI
DIRETTORE DEL MASTER DI PRIMO LIVELLO IN CYBER SECURITY

Per evitare attacchi è necessario utilizzare alcuni accogimenti I comportamenti corretti per società e dipendenti

I CONSIGLI

Sei regole da seguire sul lavoro

PER I DIPENDENTI:

1

Selezionare una buona password e non dirla a nessuno. Una buona password deve essere difficile da indovinare (e molto spesso è molto difficile da ricordare, perciò se uno se la scrive la conservi in un luogo sicuro ed eviti di incollarla con un post it al monitor...)

2

Non cliccare ciecamente su link e allegati di email

3

Fare attenzione quando si inserisce una chiavetta usb nel computer. Soprattutto nei sistemi Windows se sulla chiavetta c'è un programma, questo va automaticamente in esecuzione

DOMANDE PER IL DATORE DI LAVORO

1

E' consapevole dei rischi che corre la sua impresa e delle possibili conseguenze?

2

La sicurezza informatica viene gestita come un processo aziendale tra gli altri? E di conseguenza si stanno prendendo le misure adeguate?

3

Difficilmente un hacker attacca direttamente ma in genere cerca di entrare attraverso una porta "laterale", dal pc della segretaria per esempio. Si sta facendo un'adeguata formazione ai dipendenti, come la si fa sulla sicurezza sul lavoro o sull'antincendio?

È ACCADUTO DAVVERO

Aprì le valvole delle acque nere per vendetta

È forse il primo caso di attacco intenzionale alla sicurezza di un impianto pubblico. È il 2000, Vitek è un esperto di automazione e consulente di un'azienda che ha vinto l'appalto per l'installazione di un impianto di depurazione in Australia. Lascia per farsi assumere dall'azienda che gestisce il depuratore: la sua domanda viene rifiutata. Si vendica aprendo per 46 volte le valvole delle acque nere.