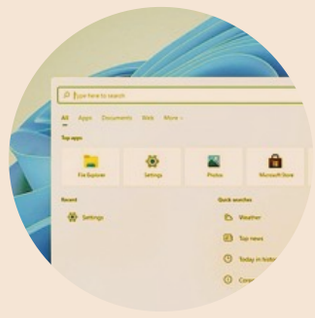
Nòva 24

In guerra la massima
«La sicurezza innanzi tutto»
porta diritto alla rovina

SIR WINSTON CHURCHILL
(1874-1965)

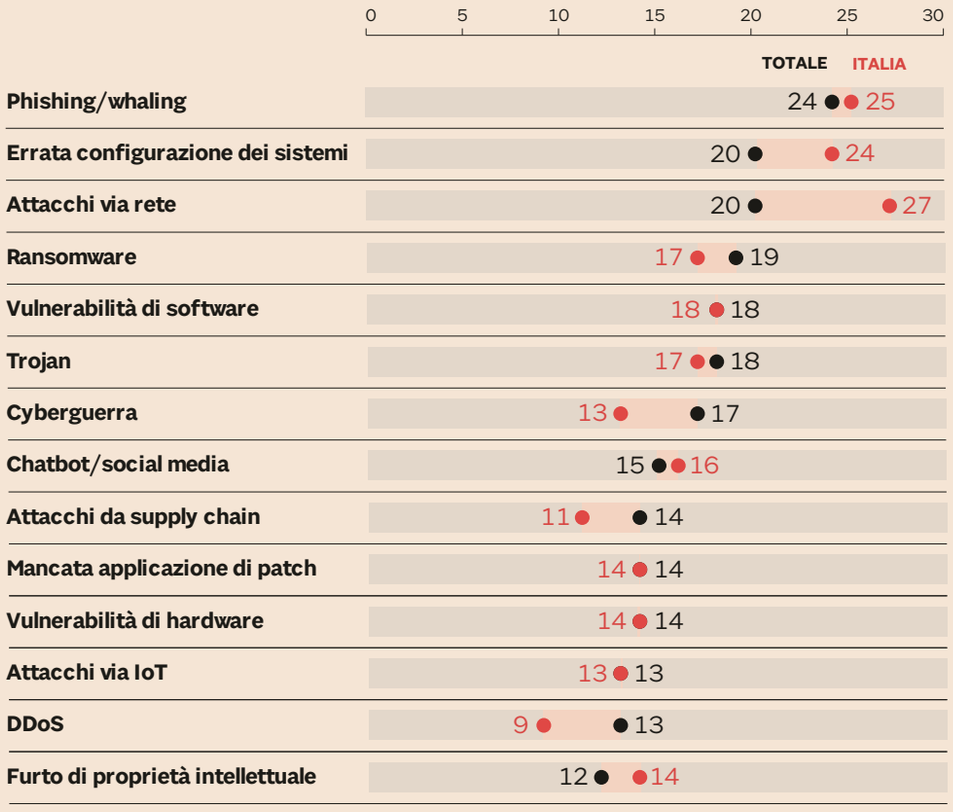


ARRIVA WINDOWS 11
Tutto quello che c'è da sapere sul nuovo sistema operativo di Microsoft che viene presentato in streaming oggi pomeriggio

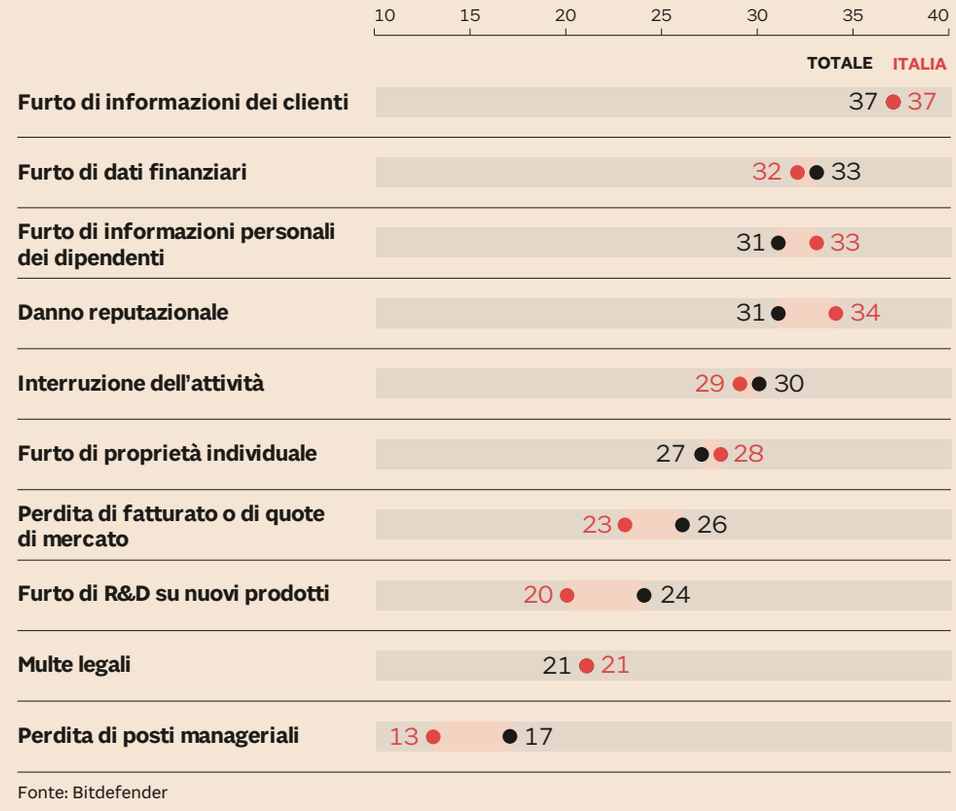
DOMENICA SU NÒVA
«Nel post-pandemia abitiamo le città, ma sogniamo la natura: consapevole delle sue fragilità l'umano cerchi nuovi equilibri»: parla la scrittrice Marta Ceroni

Conoscere i rischi di un mondo sempre più connesso

LE MINACCE PIÙ IMMINENTI
Minacce maggiori per le aziende nei prossimi 12-18 mesi. *In %, massimo tre risposte*



IL PATRIMONIO A RISCHIO
Le conseguenze più gravi in caso di attacco informatico. *In %, risposta multipla*



Fonte: Bitdefender

Scenari da cyberwar: come i conflitti globali entrano nella vita quotidiana

Sicurezza informatica. L'evoluzione della guerra informatica globale tra le grandi potenze rende sempre più vulnerabili i sistemi «civili», le infrastrutture nazionali sensibili e le aziende industriali: ecco come si sviluppa il conflitto tra le grandi potenze mondiali

Pagina a cura di
Giancarlo Calzetta

Internet ha cambiato il mondo. Lo sappiamo, ma spesso non riusciamo a cogliere quanto. Un'idea ce la possiamo fare se guardiamo a come ha cambiato gli scenari di guerra. Del resto, il progresso ha da sempre contribuito a cambiare le modalità belliche e l'indicatore più evidente è il rapporto dei morti tra soldati e civili. Nella Prima guerra mondiale, si moriva molto al fronte. Man mano che ci avviciniamo ai giorni nostri, il numero di perdite tra i soldati è andato calando mentre è esploso quello delle vittime civili: bombardamenti, guerriglia, attentati, malattie, fame... Effetti primari e secondari degli scontri che hanno spostato il bersaglio dai soldati ai cittadini. La cyberguerra non è altro che l'ultimo stadio dell'evoluzione. Non serve più rischiare la vita di personale militare per far saltare una diga, causare un incidente nucleare, sabotare un porto o avvelenare l'acqua di una città: si fa tutto via web. Ancora non abbiamo assistito a scene di distruzione di massa mediante internet, ma tutti i governi stanno già facendo le prove generali da tempo. Ci sono stati casi eclatanti come l'operazione Stuxnet, attribuita a Israele e Stati Uniti nel 2010, durante la quale furono sabotate centrifughe per arricchire uranio destinato al programma nucleare iraniano. Oppure quella che a febbraio di quest'anno ha attaccato un acquedotto in Florida modificando da remoto i livelli di idrossido di sodio fino a portarli a livelli letali. Ma la maggior parte resta, per il momento, sottotraccia. Un nugolo di operazioni nascoste della quale ci si accorge poco e tardi.

Ma cos'è esattamente la cyberguerra? Il termine indica un fenomeno estremamente ampio che implica l'utilizzo di mezzi informatici per garantire a un Governo un vantaggio di tipo economico, militare, conoscitivo o diplomatico. In pratica, si tratta di applicare le possibilità aperte dall'ampia adozione di Internet a tutte le branche delle operazioni militari: dai servizi segreti fino ai sabotatori, passando per operazioni economiche e sociali.

I pionieri di questo campo sono stati Stati Uniti, Cina e Russia che ancora oggi rappresentano le nazioni più attive, ma praticamente tutti i governi mondiali si sono attrezzati per operazioni difensive e offensive, diversificando in base ai propri interessi. «La Cina – spiega Giampaolo Dedola, membro del Great team di Kaspersky ed esperto di malware e attacchi informatici –sembra molto attiva nel settore del recupero di informazioni. Mentre altri Stati, come l'India, sembrano più interessati a operazioni svolte contro Paesi con cui sono aperte delle dispute diplomatiche o con rapporti particolarmente tesi». Negli anni, molti esperti hanno indicato la Corea del Nord come il mandante di un gran numero di attacchi portati a istituzioni finanziarie, grandi aziende ed exchange per criptovalute, ordinati per ricavare fondi in barba alle restrizioni economiche internazionali. Il più eclatante fu il tentato furto di un miliardo di dollari alla Banca nazionale del Bangladesh, riuscito solo per poco più di 80 milioni, ma sembra ci sia la loro mano anche dietro molti attacchi ransomware con richieste di riscatto milionarie indirizzate ad aziende civili.

GLI ATTORI
I pionieri sono Stati Uniti, Cina e Russia. Ma poi si sono aggiunti altri Paesi, con i loro obiettivi, sempre celati dietro anonimato

La Russia, invece, potrebbe essere specializzata in operazioni di disinformazione e nella creazione di gang criminali, un sottoprodotto del loro sistema scolastico che da tempo crea un gran numero di ottimi tecnici informatici. «Purtroppo – precisa Dedola – l'attribuzione degli attacchi è sempre molto complicata e raramente si arriva a una certezza. Una delle pratiche più importanti quando si compiono operazioni di cyberguerra è quella di nascondere la propria identità o di camuffarla. In questo caso, mentre si indaga ci si imbatte in falsi indizi che puntano ad addossare le colpe a gruppi o Paesi che non sono coinvolti». Quindi, se è facile fare la conta delle operazioni informatiche, è meno semplice capire chi c'è dietro. L'unica cosa certa è che non esistono più nazioni escluse dal gioco.

Servono strumenti adeguati per la difesa: «L'Italia non può dipendere dall'estero»

Strategia
Politiche industriali

Ogni esercito ha due fronti da tenere ben presenti quando si prepara una guerra: l'attacco e la difesa. La stessa cosa vale nel caso delle guerre informatiche, ma con un distinguo importante: mentre per attaccare i bersagli si può fare affidamento su strumenti costruiti "in casa" e su di un ampio arsenale disponibile sia gratuitamente sia a pagamento, per la difesa le cose sono molto più complesse. Se durante un attacco le armi si rivelano inadeguate, l'attacco fallisce e si può riprovare. Se invece non si hanno le difese adeguate, le conseguenze possono diventare devastanti. Purtroppo difendere in maniera appropriata un'azienda o un'entità governativa è molto più difficile che attaccarla e una delle pratiche più importanti è quella di strutturare la difesa "a buccia di cipolla", ovvero predisponendo strati diversi che si occupano di contrastare gli attacchi a diversi livelli. Il primo deve impedire ai pirati di entrare, ma se questo viene superato, altre tecnologie devono intervenire e analizzare quello che succede nella rete per rilevare eventuali intrusi. Se le cose vengono fatte per bene, portare a segno attacchi diventa molto difficile, ma esiste sempre un limite: se il software che usiamo per difenderci non è prodotto nel nostro Paese, può sempre essere esposto alle pressioni e azioni aggressive del governo d'appartenenza.

CATENE DIFENSIVE
Nicola Mugnato (Gyala): «In fatto di sicurezza informatica non ci si può fidare di nessuno: cruciale avere software italiano»

«Almeno un anello della catena difensiva – dice Nicola Mugnato, founder e general manager di Gyala, una delle poche aziende che producono software di difesa informatica in Italia – deve essere fatto in Italia perché in fatto di sicurezza informatica non ci si può fidare di nessuno». La sua accusa ha radici ben solide. A inizio 2020, per esempio, è stata scoperta l'operazione Rubicon, un accordo tra Germania e Stati Uniti che permetteva ai due Paesi di spiare i documenti crittografati dei loro stessi alleati (tra cui l'Italia). A fine maggio di quest'anno, invece, si è scoperto che la Danimarca ha aiutato gli Usa a spiare alcuni politici europei. «Per la difesa informatica dobbiamo dipendere in larga parte da software straniero – dice Mugnato - perché al momento non esiste una filiera italiana in questo senso. Nel nostro Paese ci sono moltissime aziende con grandi competenze nel settore, ma forniscono servizi usando comunque prodotti che arrivano dal'estero. Sarebbe, invece, vitale poter fare affidamento su un'offerta italiana più ampia».

Ma la situazione è complessa. Al giorno d'oggi è molto più semplice creare un'azienda che fornisca servizi piuttosto che una in grado di sviluppare software molto complesso. Servirebbero stimoli e supporti a livello governativo per creare una sicurezza nazionale più robusta.

L'analisi

NESSUNO OGGI PUÒ RITENERSI AL SICURO

Quando si parla di attacchi informatici, si crede che i bersagli siano solo grandi aziende o personaggi importanti. Tanto più per la cyberguerra. Ma non è così! Al giorno d'oggi nessuno può pensare di essere al sicuro perché «poco interessante». Innanzitutto perché la maggior parte degli attacchi è automatica e condotta "a strascico". Ci sono bot che scandagliano la rete in cerca di vittime senza fare alcuna distinzione. Molti casi di ransomware colpiscono piccole aziende o singoli professionisti. In secondo luogo, nessuno di noi può sapere come è connesso con gli interessi degli attaccanti. Per attaccare entità ben protette si usa prendere di mira un fornitore, entrare nei suoi computer e studiare un modo per raggiungere il vero bersaglio. Quindi basta lavorare per un'azienda che ha clienti importanti e si finisce nel mirino. Una ricerca di Bitdefender indica che ben il 47% degli It manager italiani crede che la cyberguerra possa coinvolgerli in qualche modo.

Ma chi dobbiamo temere? Le operazioni di cyberguerra vengono condotte da gruppi di hacker chiamati Apt, dall'inglese Advanced and Persistant Threat (minaccia avanzata e persistente). Il loro ecosistema è molto vario. Ci sono Apt che dipendono direttamente dai governi e organizzazioni criminali indipendenti che possono fornire i loro servizi a entità governative. Sono molto esperti e spesso dispongono di risorse imponenti per celare molto bene il loro operato. Per esempio, il gruppo Turla, che si crede essere collegato al governo russo, in passato usava una distribuzione via satellite di Internet per nascondere la posizione dei loro server, rendendoli impossibili da localizzare. L'Equation Group, collegabile a una realtà anglofona, è specializzato nel lasciare pochissime tracce. Delle loro numerose operazioni, sono pochissime quelle intercettate mentre erano ancora in corso e della maggior parte si trovano solo indizi che non permettono di risalire ad altro che al loro modus operandi. Barium, Apt collegato alla lingua cinese, sembra essere connesso all'attacco ShadowHammer, operazione che si è servita della violazione del sistema di aggiornamento dei computer Asus (milioni di download) per colpire un ristretto numero di Vip identificati tramite indirizzo Mac recuperati durante una precedente operazione mai scoperta.

Se il nostro nemico è un governo, abbiamo poche possibilità di farla franca, e Giampaolo Dedola di Kaspersky dipinge un futuro in cui le cose diventeranno ancora più difficili da fronteggiare: «Negli ultimi anni sono emersi molti nuovi Apt, soprattutto in Medio Oriente, Asia Centrale e Asia meridionale. Già oggi la cyberguerra non si può più restringere alle tre "potenze" tradizionali di Cina, Russia e Usa».

VkVSlyMjNGY3ZWNhYzAtOGVhNi00OGZmLWJhOTQtODMyODdkYzZkZDllIyMjMDAwMDAtMDAwMC0wMDAwLTAwMDAtMDAwMDAwMDAwMDAwIyMjMjAyMS0wNi0yNFQwOTo0MjowNSMjI1ZFUg==