Un aspetto dell'essere umano che questa pandemia ha mostrato è la sua difficoltà a comprendere la pericolosità di alcuni fenomeni che per loro natura presentano un'evoluzione nel tempo di tipo esponenziale. Come c'insegnano gli studiosi di economia comportamentale, la scienza a cavallo tra l'economia e la psicologia che ha dato numerosi premi Nobel, l'essere umano capisce meglio i fenomeni che hanno un'evoluzione nel tempo di tipo lineare ovvero quelli che rispondono a uno stimolo d'ingresso con una reazione proporzionale a esso: la metà se si dimezza, costante se rimane invariato, il doppio se raddoppia, il triplo se… e via così.
Chiunque abbia potuto disegnare una curva esponenziale in un grafico avrà visto come nei primi istanti la crescita nel tempo rimane inferiore a quella di una data curva lineare. Per questo si fatica a capire perché ci si dovrebbe preoccupare se la crescita è inferiore a un tasso proporzionale che si giudica "piccolo". Indiscutibilmente tutto diventa chiaro quando l'accelerazione impressa dalla dinamica esponenziale mette tutti di fronte al disastro determinato delle dinamiche esponenziali che si scatenano quando le superficie d'attacco non sono costantemente monitorate e contenute.

Nel caso del Covid-19 la superficie d'attacco è rappresentata dal numero di contatti tra le persone che è stato ridotto con le misure di distanziamento sociale. Nel caso della cyber security, invece, la superficie d'attacco dei software malevoli – detti anche *malware* – è rappresentata dai numeri di contatti che i computer o gli oggetti intelligenti connessi alla rete aziendale instaurano

impropriamente con il mondo esterno e che possono essere facilitati da comportamenti non corretti da parte dei dipendenti.
Se in tempi normali ridurre la superficie d'attacco di un'azienda è una pratica che dovrebbe essere tra le priorità per chi è chiamato a ruoli di responsabilità gestionale della rete informatica e non solo, lo diventa ancora di più adesso, finito il periodo di lockdown. Infatti, molte aziende continuano a ricorrere per tutte quelle mansioni per cui è possibile, a modalità di telelavoro o *smart working*. Permettere l'uso di dispositivi da remoto per garantire la continuità lavorativa aumenta dal punto di vista della sicurezza informatica, la superficie d'attacco.
In un ambiente come quello domestico, lo *smart working* fa aumentare comportamenti "pericolosi", come la lettura di un allegato a un'email che sembra del tutto legittima perché si presenta come inviata da un mittente conosciuto o comunque di cui ci si fida. La probabilità che questi comportamenti siano avvenuti in perfetta buona fede è proporzionale al numero di campagne di email mirate lanciate dai cybercriminali.
Recentemente è stato pubblicato uno studio da parte di una delle più grandi aziende al mondo di antivirus, la rumena Bitdefender, che ha misurato come sulle reti internet delle varie nazioni occidentali le campagne di email con allegati pericolosi a tema coronavirus siano avvenute in coincidenza con i momenti di picco dell'emergenza. I cybercriminali hanno senza dubbio tentato di sfruttare un momento di fragilità psicologica delle persone per installare nelle loro macchine dei *malware* o comunque *software* che permettono di sfruttare illecitamente le risorse dei computer come *adware* o *cryptominer*.
Gli *adware* che permettono il monitoraggio dell'attività online e i *cryptomining malware* che sfruttano in maniera parassita le capacità di calcolo del computer ospitante consumando fraudolentemente l'elettricità, non sono malevoli di per sé, tuttavia le loro vulnerabilità potrebbero essere sfruttate da parte dei cybercriminali successivamente alla loro installazione per accedere alla rete aziendale. Per questo vanno individuati e rimossi il più presto possibile.
Una società italiana, Talaia Solutions, che in collaborazione con Bitdefender offre una soluzione innovativa di individuazione della presenza di malware o sofware pericolosi attraverso l'osservazione del traffico della rete aziendale, ha notato un aumento di segnalazioni della presenza di *adware* e *cryptominer* nella fase due che vede il lento ritorno delle macchine da casa in ufficio. L'ingegnere Enrico Guidi fondatore e responsabile commerciale di Talaia mi racconta che, grazie all'intelligenza artificiale del loro sistema e a un monitoraggio aggiornato ogni sessanta minuti dei siti di tutto il mondo temporaneamente compromessi, sono riusciti a individuare subito i sistemi compromessi evitando gravi danni economici e di immagine per

l’azienda.

Com’è noto, con l’approvazione della legislazione europea per protezione dei dati personali che va sotto il nome di GDPR ogni azienda ha l’obbligo ora di comunicare al garante ogni compromissione della rete aziendale che ha permesso l’accesso fraudolento a dati sensibili. L’industria della sicurezza informatica italiana ha creduto che il mercato italiano si facesse più attento alla necessità di dotarsi dei necessari strumenti per evitare di trovarsi in situazioni generate dal fatto che la superficie di attacco non veniva costantemente ridotta. Purtroppo, non è stato così. Parlando anche con altre aziende attive nel settore, questo scenario fatica ad avverarsi e l’unico impatto della GDPR è che possiamo leggere, e leggeremo sempre più, quanto si dimostrino poco coscienti del problema coloro che occupano ruoli di responsabilità nella gestione delle aziende italiane. Poco prima dello scoppio della pandemia ha fatto scalpore un’azienda dell’Emilia Romagna che aveva avuto i suoi dati bloccati da un *ransomware* e che s’era pubblicamente pronunciata contro il pagamento del riscatto richiesto di qualche milione di euro. L’atteggiamento di non trattativa fu lodato dalla stampa ma sarebbe stato interessante chiedere quale fossero stati fino a quel momento il livello di spesa e la consapevolezza di cosa significhi fare sicurezza informatica.

Oltretutto la presenza di un *malware* come un *ransomware* indica che tutto l'ecosistema dei fornitori e dei clienti è stato messo a rischio. Per questo motivo il nuovo regolamento prevede l'obbligo di denuncia e la nomina di un responsabile dei dati. Purtroppo nella maggioranza delle aziende si vive tutto ciò come un puro adempimento burocratico e non come occasione per comprendere il vero valore di tutte queste norme: la salvaguardia del sistema economico del paese. Sfortunatamente, senza un management o una proprietà consapevoli dei rischi che seguono curve evolutive nel tempo di tipo esponenziali, come quelli generati dalla presenza di un *malware*, si ragiona ancora con la logica di gestione dei rischi derivanti da processi lineari.
L'ingegnere Giovanni Anceschi, co-fondatore di Yoroi, un'altra società italiana di cyber security racconta a *ytali* di come poco prima della pandemia una grande azienda attiva in un importante settore del *made in Italy* – cucine componibili – li avesse chiamati perché a un certo punto le macchine a controllo numerico eseguivano delle operazioni sbagliate e intere giornate di produzione venivano distrutte. Gli specialisti di sicurezza informatica intervenuti hanno scoperto la presenza di un malware e proceduto a bonificare le macchine.
L'azienda, pur avendo vissuto questa esperienza con tutti i suoi danni, davanti alla proposta di installare un servizio di monitoraggio continuo il cui scopo sarebbe stato quello di ridurre la superficie d'attacco ha risposto che preferiva pagare solo per l'intervento perché tanto la probabilità che sarebbe successo ancora, a loro parere, era bassa.
Purtroppo non è un caso raro. Questo e altri casi simili hanno un unico grande comun denominatore: il credere di avere a che fare con fenomeni lineari e sporadici e che possono essere risolti con una logica lineare. Ma non è così. L'azione e il successo dei cybercriminali si nutrono di quest'atteggiamento. Senza la presenza di servizi di protezione adeguati nei prossimi mesi, *malware* o *sofware* pericolosi, installati per sbaglio nelle macchine durante lo *smart working*, apriranno le reti aziendali alle azioni di cybercriminali.

Cyber security, antivirus, hackers and malware concepts with secure laptop at center

Al momento le aziende italiane incontrano gravi difficoltà per quanto riguarda la gestione di cassa ed è facile dire che ci sono ben altri problemi da affrontare piuttosto che la sicurezza informatica. Non è così. Garantire la protezione informatica dalle aziende riducendo in maniera attiva e costante la superficie d'attacco, e non reagire, spesso male, solo dopo che "i buoi sono scappati dalla stalla", è la chiave per garantire una ripresa economica sostenibile.

Sarebbe auspicabile, allora, che la task force del governo guidata da Vittorio Colao mettesse in chiaro che anche la protezione informatica o cybersecurity è fondamentale per la ripresa vincolando l'uso di eventuali aiuti a maggiori investimenti in questo campo. Vittorio Colao stesso dovrebbe conoscere bene i danni legati all'installazione di *malware* perché fu al centro di un caso di sottrazione di documenti confidenziali dal suo computer dopo aver installato erroneamente un allegato di una mail che credeva provenire legittimamente dal servizio IT dell'azienda di cui era il capo.

Grazie al tuo sostegno

y*tali* sarà in grado di proseguire le pubblicazioni nel 2020.

Clicca qui per partecipare alla raccolta fondi.

Your support will give *ytali* the chance to carry on in 2020.

Click here to contribute to the fundraising.

Votre soutien donnera à ytali *la chance de continuer en 2020.*

Cliquez ici *pour contribuer à la collecte de fonds*.