Conversazione con Deanna House a cura di Martina Saltamacchia

photo © Fly D_Unsplash

Supremazia digitale

La cybersecurity nella guerra dei mondi

Siamo nel pieno di una serie di battaglie informatiche su scala globale. La divisione del mondo in blocchi contribuisce a un inasprimento degli attacchi. A tutti i livelli. I Paesi sono impegnati a investire massicciamente su questo insidioso terreno. La formazione, vieppiù sofisticata, è fondamentale. Negli USA, come è facilmente intuibile per il ruolo che quel Paese ricopre sulla scena mondiale, l'impegno in cybersicurezza è massiccio: dai primi percorsi di alfabetizzazione tecnologica nelle scuole a interventi sempre più impegnativi e decisivi. In gioco vi è la partita della sicurezza nazionale. E la sicurezza informatica è una forma di difesa che è anche attacco. Intervista a una grande esperta, la professoressa Deanna House dell'università Omaha, Nebraska.

La cybersecurity è un tema sempre più impattante nella vita di tutti. In modo particolare investe i governi mondiali. Non passa giorno senza che arrivi la notizia di qualche attacco informatico. Quel che un tempo poteva sembrare fantascienza, da qualche anno è più che una realtà. Una "questione grattacapo" per i Paesi, specie in fasi storiche assai complesse e ad alta tensione come quella che il mondo post globalizzato sta oggi affrontando. Ci aiuta a comprendere il significato di tale sfida Deanna House, insegnante e ricercatrice universitaria. I suoi campi di ricerca riguardano gli aspetti comportamentali della cybersecurity e le misure protettive e preventive adottate da utenti, governi, forze armate e organizzazioni. Un'accademica impegnata nella formazione della "prima linea"

Qual è lo stato attuale della cybersecurity e come sta cambiando?
Uno degli aspetti forse più interessanti della cybersecurity è che è in continua evoluzione. Abbiamo visto molte cose sorprendenti nell'ultimo decennio, o anche nell'ultimo anno, e continuiamo a vederne di nuove – aree che non sono mai state prese di mira prima, attacchi che non sono mai stati fatti prima. Ad esempio, ultimamente, sono stati presi di mira iOS e Apple; e ho letto di attacchi rivolti al sito Internet of Things (IoT), ovvero tutti quei dispositivi informatici in grado di raccogliere e trasferire dati su una rete wireless senza bisogno dell'intervento umano.

Sono notizie che colpiscono molto le persone che utilizzano quotidianamente la tecnologia, e creano grande apprensione in chi non sa molto di cybersicurezza. In genere, dal punto di vista dell'utente domestico, le persone non adottano un'ottima igiene informatica. Per esempio, non installano con regolarità le nuove patch software per correggere eventuali vulnerabilità, man mano che vengono scoperte e sono spesso all'oscuro di attacchi in corso, eccetto quando vengono contattati da un'azienda che li mette al corrente dell'attacco subito, il che non è molto frequente. Personalmente, io vivo su Twitter ed è lì che ottengo la maggior parte delle notizie al proposito, ma questo è uno spazio in continua evoluzione e per i non addetti ai lavori è difficile ottenere informazioni.

Quali sono le principali sfide che la cybersecurity si trova oggi ad affrontare?
Con la globalizzazione, siamo diventati tutti iperconnessi. È nata l'esigenza di avere aziende con sedi in tutto il mondo, 24 ore su 24 e, di conseguenza, la necessità ininterrotta di comunicazione. Questo ci ha spalancato grandi opportunità, ma anche prestato il fianco a molte nuove vulnerabilità; l'utilizzo di molteplici dispositivi a cui siamo così vincolati, come la dipendenza dalla comunicazione digitale e dai messaggi di testo, ci aprono a infinite possibilità di essere attaccati.

Nella mia ricerca mi occupo di behavioral cybersecurity (sicurezza informatica comportamentale), dell'elemento umano e, quindi, sono consapevole di quanto siamo tutti vulnerabili come persone. Scherzo sempre sul fatto che un giorno anch'io subirò un attacco: qualcuno mi invierà un'e-mail, sarà davvero credibile e io ci cliccherò sopra, senza accorgermene. Non ci si può aspettare che si sappia sempre se la comunicazione che ti raggiunge è legittima o meno. E questo crea molte problematiche.

Un altro fattore che complica il quadro è rappresentato dai potenziali introiti. Un cyber attaccante può guadagnare cifre astronomiche, per cui ci si trova a dover combattere con persone che chiedendo un riscatto a un'azienda potrebbero guadagnare milioni di dollari. E, di solito, gli attacchi ransomware partono dall'uomo.

In questo contesto, qual è l'impatto di ChatGPT?
Al momento mi sembra che per lo più stiamo usando ChatGPT per scopi utili, ma ci sono già cyber attaccanti malintenzionati che lo usano per creare messaggi email che appaiono assolutamente legittimi, privi di errori ortografici e grammaticali. C'è anche chi sta già cominciando a scrivere attacchi informatici tramite ChatGPT, chiedendo al chatbot: "come posso scrivere un attacco ransomware utilizzando ChatGPT?", "come posso scrivere un worm?"

Attualmente stiamo conducendo un progetto di ricerca sul tema del sospetto nelle e-mail. Uno degli impegni che ci siamo assunti è quello di addestrare i destinatari delle email a essere più sospettosi e, per farlo, stiamo cercando di approfondire gli aspetti che aiutano l'utente a determinare se qualcosa è legittimo o illegittimo. In parte si tratta di parole comuni: stiamo analizzando un enorme set di dati sulle email, cercando di individuare i trend ricorrenti, per esempio osservando il modo in cui le parole sono disposte nel corpo del messaggio. In un altro progetto correlato, ho esaminato la gentilezza nelle email di phishing, osservando il linguaggio e cercando di capire se il tono cortese potesse essere un fattore per determinare l'autenticità dell'email.

Torniamo alla dimensione globale. Data l'importanza crescente della sicurezza informatica nel mondo, la cybersecurity è diventata probabilmente ancora più cruciale della difesa bellica tradizionale. Quali misure si stanno adottando per affrontare queste sfide?
Il ruolo crescente della cybersecurity nel mondo di oggi pone molte sfide perché, invece di dover stare a guardare chi possiede armi nucleari, ora ogni Paese in possesso di capacità informatiche ha voce in capitolo. E questo comporta una maggiore complessità: dal punto di vista bellico, non si tratta solo di Paesi potenti, ma di qualsiasi Paese che disponga di un team informatico o di un team da ingaggiare per svolgere attività dannose. Questo crea anche sfide legate all'attribuzione, ad esempio la possibilità di sapere chi ti sta realmente attaccando e, di conseguenza, un Paese attaccato potrebbe avere tutto l'interesse a far sembrare che l'attacco sia stato sferrato da un suo certo nemico.

Come possiamo affrontare queste sfide? Abbiamo bisogno di accademici, di ricercatori che si occupino di questi problemi, perché i militari dei Paesi e i professionisti del cyber sono già impegnati ad affrontare altre priorità. Si tratta di mansioni strategiche per rispondere a problemi complessi, un mix di opportunità e responsabilità per i ricercatori. A proposito del mio ruolo,

mi ci vogliono tre anni per condurre una ricerca e, alla fine, non arrivo a comprendere tutto. Tuttavia, credo che chi si misura con progetti di questo tipo possa fornirci idee importanti per essere proattivi e, così, escogitare correttivi e soluzioni prima che un attacco cyber su larga scala vada a colpire l'intera popolazione globale.

Quali misure può adottare un Paese per garantire la sua supremazia digitale?
Da una parte, abbiamo alcuni top player storici che cercano di mantenere la loro supremazia digitale, mentre, allo stesso tempo, si affacciano sulla scena nazioni emergenti assai agguerrite. Per garantire la supremazia digitale è necessario continuare a promuovere la tecnologia tra i nostri figli, dando loro l'opportunità di conoscere e maturare familiarità con la tecnologia e la sicurezza informatica fin dai primi anni di vita.

All'Università del Nebraska, a Omaha, sono co-investigatrice principale di un seminario di cybersecurity per ragazze delle scuole medie finanziato dalla National Security Agency. Questo è uno dei tanti seminari che si svolgono negli Stati Uniti, dove si insegna ai giovani la cybersicurezza; e ci sono realtà simili in tutto il mondo che permettono agli studenti di imparare la tecnologia e di aggiungerla alla lista delle proprie competenze.

Gran parte della nostra forza lavoro non è esperta in tecnologia, non è addestrata alla sicurezza informatica. Questo è un problema. Imparare a codificare un software è come imparare una nuova lingua e il suo funzionamento; ma apprendere in giovane età è molto più facile che non quando si è adulti e, improvvisamente, ci si trova nella necessità di imparare una nuova lingua.

Ma non si corre anche il rischio di effetti negativi esponendo i giovani fin da piccoli alla tecnologia informatica? Dove si trova l'equilibrio tra il tentativo di diffondere il più possibile l'uso della tecnologia digitale e tutti i danni che ne possono derivare?
Di recente, assieme a un collega canadese e a un collega scozzese, ho condotto una ricerca sulla privacy dei ragazzi. Per cercar di capire quale sia la cosa migliore per loro, abbiamo esplorato diverse prospettive, esaminando la letteratura tecnologica, la sicurezza della rete e ciò che i pediatri dicono sull'uso di Internet e sulla privacy. Siamo partiti dalla convinzione che sia davvero responsabilità di ciascuno proteggere i propri figli e che i ragazzi stessi debbano avere voce in capitolo, ma fino a una certa età sono ancora una fascia vulnerabile della popolazione, e quindi dobbiamo dare l'esempio come società.

È importante che siano messi nelle condizioni di poter scegliere, ma la scelta deve essere adeguata all'età. Non do ai miei figli un telefono con accesso a Internet lasciandoli liberi, pensando che non finiranno nei guai, perché invece lo faranno. Invece, intavolo con loro una conversazione onesta, dicendo loro che non posso mettermi a controllare tutto quello che fanno e vedono, ma che ci sono pagine su cui possono arrivare e che, in tal caso, confido che siano in grado di fare la scelta migliore per loro e che non finiscano a guardare cose (e spiego nello specifico quali sono) che alla loro età non dovrebbero guardare. I ragazzi vanno sempre a mettersi nei guai e, quindi, mantenere una conversazione aperta è probabilmente il metodo migliore anche se, ovviamente, è una sfida.

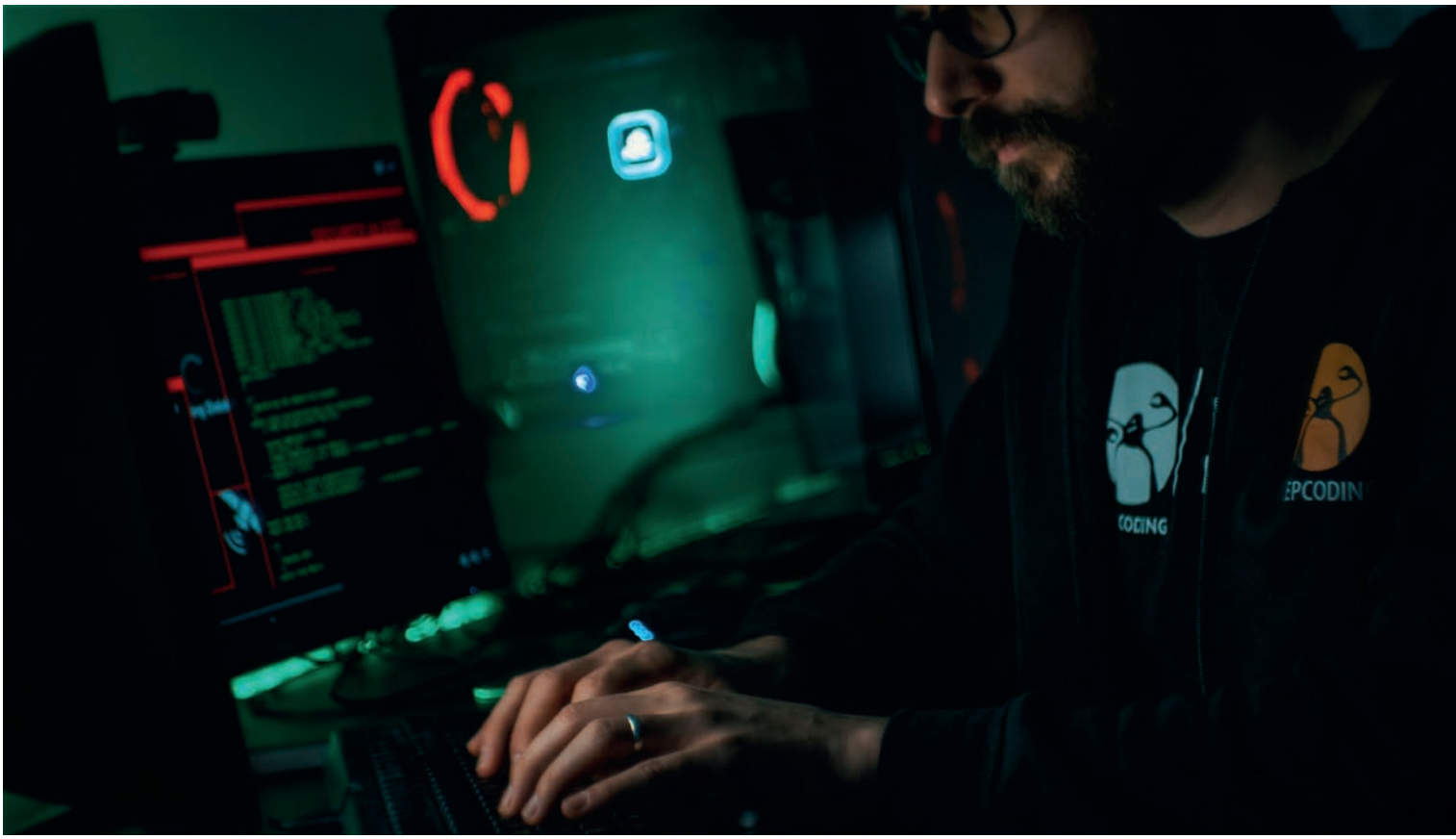
Lei lavora come ricercatore presso il National Counterterrorism Innovation, Technology, and Education Center (NCITE), il Centro di Eccellenza del Dipartimento di Sicurezza Nazionale americana per la prevenzione del terrorismo e la ricerca sull'antiterrorismo. Può parlarci in breve dell'attività del centro?
Il consorzio NCITE, che ha sede presso l'Università del Nebraska a Omaha, comprende più di 50 ricercatori provenienti da 19 istituzioni diverse degli Stati Uniti e dell'Europa. I ricercatori NCITE hanno un'ampia gamma di competenze e di background accademici: scienze politiche, criminologia, psicologia, sociologia, economia e tecnologia dell'informazione. Combinando

prospettive e metodi di diverse discipline, NCITE affronta i problemi in modo innovativo e fornisce soluzioni inedite per le complesse questioni di sicurezza nazionale, aiutando la prima linea della difesa a proteggere il Paese generando intuizioni di ricerca uniche, costruendo strumenti innovativi e progettando programmi accademici per rafforzare la forza lavoro. Alcuni esempi di quel che svolgiamo al NCITE includono la valutazione delle minacce alla sicurezza nazionale poste dall'adozione del metaverso; l'uso dell'apprendimento automatico per anticipare gli eventi di estremismo violento; l'intervista a familiari di estremisti violenti sotto accusa per gli attacchi, allo scopo di scoprire le lacune del sistema; la mappatura delle tattiche, delle tecniche e degli obiettivi dei gruppi di estremisti violenti.

In che modo NCITE sta affrontando le sfide poste dalla cybersicurezza?
In uno dei nostri ultimi progetti, ho lavorato insieme a Michelle Black e Lana Obradovic alla ricerca sulla formazione e l'istruzione specifica per il sistema di intelligence della Sicurezza Nazionale americana, individuando dapprima le competenze fondamentali per gli agenti di controspionaggio e poi intraprendendo un approfondimento specifico in materia di cybersecurity e tecnologia particolare per gli agenti di controspionaggio. Abbiamo intervistato persone che lavoravano in aziende, sia del governo che del settore privato, per scoprire come imparano, come acquisiscono conoscenze, come aumentano le loro competenze in materia di tecnologia e sicurezza informatica.

E quali sono stati i risultati del vostro progetto?
Probabilmente non è una sorpresa, ma ciò che è emerso dal nostro studio è che il settore privato investe e pone più enfasi sul mantenimento e sull'aumento delle competenze dei propri dipendenti, facendoli partecipare a corsi di formazione particolarmente creativi e stimolanti. Abbiamo anche scoperto che la maggiore o minore conoscenza tecnologica sul posto di lavoro dipende dagli anni della laurea; cioè, se ci si è laureati da più tempo, ecco che si parlerà di mainframe mentre, se la laurea è più recente, si parlerà di IA e si conoscerà la business analytics, la cybersecurity, e così via.

photo © Keepcoding_Unsplash



Ci siamo proposti di trovare un modo per fornire una sorta di tabella di marcia delle competenze di base per gli agenti del controspionaggio, rivolgendoci alle persone che escono dall'università e iniziano a lavorare, fornendo loro una preparazione di base seguita da piani formativi più evoluti che consentano di intraprendere – se lo desiderano – un percorso tecnologico o di cybersecurity più approfondito; ma, allo stesso tempo, pensiamo alla forza lavoro già in attività, a come riqualificarla e aggiornarla in materia di tecnologia e cybersecurity. Per garantire la supremazia digitale di cui parlavamo prima, questo tipo di formazione è davvero necessario, a tutti i livelli. Se pensiamo alle aziende, ai settori governativi, alle infrastrutture critiche, al settore privato, abbiamo bisogno di specialisti con profonde competenze specifiche. Ma oggi è diventato indispensabile che tutti si abbia una conoscenza della cybersecurity e della tecnologia.

Deanna House, PhD, è Assistant Professor presso il dipartimento di Information Systems & Quantitative Analysis dell'Università del Nebraska a Omaha, e ricercatrice presso il National Counterterrorism Innovation, Technology, and Education Center (NCITE). I suoi interessi di ricerca riguardano gli aspetti comportamentali della cybersecurity e le misure protettive e preventive adottate da utenti, governi, forze armate e organizzazioni.