FONDAZIONE BRUNO KESSLER
MAGAZINE

Eserciti di bit

10 Maggio 2023

Fra i protagonisti di #WNF23, Silvio Ranise, direttore del Centro per la Cybersecurity di FBK e professore di Informatica dell'Università di Trento, per parlare di attacchi cyber e dei loro effetti anche nel mondo reale, insieme a Riccardo Meggiato, consulente in digital forensics e cybersecurity

Moderati dal giornalista Luca Zorloni di Wired, Meggiato e Ranise hanno alternato considerazioni pratiche e distinguo teorici per introdurre alcuni aspetti chiave dell'evoluzione della cybersecurity.

In primo luogo Meggiato ha accennato al fatto che gli attacchi informatici attuali sono il frutto di strategie sempre più complesse che richiedono tempi assai lunghi di preparazione e di conseguenza una attività molto consistente di studio delle reti da parte degli attaccanti. In gergo, quella che viene definita "Cyber kill chain", la scansione delle fasi di pianificazione di un attacco, comprende una serie di passaggi preparatori cui segue l'azione di attacco vero e proprio (cosiddetta delivery) e, in caso di successo, gli effetti.

Sollecitato dal moderatore a proposito dell'attualità e in particolare con riferimento al possibile impiego di Chat Gpt per potenziare il cybercrimine, Ranise ha constatato il fatto che questa nuova tecnologia permetta sì di sofisticare gli attacchi, rendendoli più scalabili ed efficaci, ma ha anche ricordato come gli stessi strumenti possano essere utilizzati come rimedio. Fortunatamente non esiste solo la dark side, poiché le stesse tecnologie sono a disposizione degli ethical hackers per fare ad es. "penetration testing", ossia per simulare attacchi e mettere alla prova le vulnerabilità dei sistemi, vulnerabilità che, una volta spiegate, si possono poi curare.

A partire dalla domanda se sia l'essere umano l'anello debole della catena i relatori hanno rimarcato quanto conti la componente psicologica / sociale, lanciando un monito: la centralità della cybersecurity nel discorso pubblico non deve ingannarci, sebbene sia apparentemente aumentata la consapevolezza, bisogna tener conto degli errori umani e soprattutto non dobbiamo pensare che gli attacchi siano rompicapi di semplice soluzione.

Emerge a riguardo il tema della competenze, che nella filiera della conoscenza si articola a partire dalle opportunità formative offerte alle scuole superiori e prosegue con gli studi universitari, così avviene la formazione e l'esposizione alla ricerca in FBK. Competenze e consapevolezza molto più diffuse sono fondamentali. Questo implica una questione di cultura della cybersecurity che scongiura nuove "horror stories" generate da una configurazione poco attenta. Se, ad esempio, un amministratore di sistema mette in funzione un servizio su Internet – commenta Ranise – ponendo

attenzione solo all’efficienza e alla scalabilità non curando la sicurezza, aumenterà sensibilmente il rischio di attacchi. Per questo occorre creare competenze di base e avanzate, ad es. sulla crittografia teorica e applicata, in maniera diffusa tra la più larga fascia possibile di esperti in Information Technology (IT).

Per la crittografia in particolare devono essere sviluppate sia competenze teoriche che applicate. Esiste infatti uno squilibrio enorme fra “algoritmo su carta” e relativa implementazione. L’esempio riportato è quello di un uso con parametri sbagliati che rende nullo l’uso di tali tecniche e fornisce un falso senso di protezione.
Se il cybercrime corre, diventa sempre più difficile tenere il passo aggiornandosi. Diventa così sempre più utile un’offerta formativa che si ponga fra la formazione universitaria e il mondo del lavoro, perché alle aziende servono persone con competenze in cybersecurity capaci di applicarle in tutti i contesti.



Un ulteriore elemento di complicazione del quadro è l’introduzione del calcolo quantistico per sgretolare la protezione offerta dalle tecniche crittografiche usate attualmente per garantire la riservatezza, l’integrità e l’autenticità dei dati scambiati su Internet.
Su questo aspetto, prendendo in considerazione la complessità del fenomeno e la necessità di coordinamento fra vari attori globali per giungere gradualmente a standard condivisi, Ranise ha rassicurato gli intervenuti affermando che ci vorrà ancora qualche anno per aver computer quantistici in grado di decrittare secondo nuove logiche.

La crittografia usata oggi ovunque è basata sulla difficoltà di risolvere un problema matematico (che richiede anni). In teoria i nuovi computer quantistici saranno in grado di risolvere gli stessi quesiti in minuti o addirittura secondi, ad es. scovando chiavi di cifratura oppure intaccando l’integrità, ossia permettendo agli attaccanti di cambiare le caratteristiche delle operazioni senza lasciare segni, come se fossero state realmente prodotte dai titolari attaccati con successo.

La comunità internazionale della ricerca in cybersecurity è coinvolta in uno sforzo sociale enorme per rendere gli algoritmi sempre più robusti. In tal senso, si è cominciato a parlare di crypto agility, ossia della possibilità di sostituire algoritmi crittografici più velocemente possibile, salvaguardando la sicurezza. In particolare, per quanto riguarda le imprese, sarà necessario passare da un approccio reattivo a uno anticipante, considerando la pianificazione degli aggiornamenti come un aspetto ineludibile.

In chiusura Ranise ha menzionato l'esperienza di SERICS, iniziativa in tema di cybersecurity che unisce gli apporti del mondo della ricerca e delle imprese grazie alle risorse ingenti messe a disposizione dal Pnrr e che promette di far fare al sistema paese un salto di qualità, puntando su un approccio interdisciplinare per migliorare il cloud, l'identità digitale, la consapevolezza e la compliance in conformità a regole provenienti da altri settori a loro volta in rapida evoluzione come



Nella stessa giornata del festival, domenica 7 maggio 2023, si è tenuto anche il Workshop "La cybersecurity non è solo roba da nerd" che ha visto intervenire il ricercatore del Centro FBK-Cybersecurity Matteo Rizzi, insieme a Elisa Rapetti di Edi onlus e Carmelo Ferrante di digitalforensics.it

I tre relatori hanno fatto un affresco dei cyber rischi in particolare per quanto riguarda i minori, concentrandosi soprattutto sul child grooming – tecnica manipolatoria per creare una relazione affettiva – sessuale, che si articola in 5 fasi: amicizia, risk assessment, costruzione del rapporto di fiducia , fase dell'esclusività (isolare, ecco la violenza del grooming, fatta di controllo e umiliazione), e infine relazione sessualizzata (con foto per ricattare e/o indurre incontri offline).

In Italia è reato dal 2012, non è necessario l'incontro offline come fattispecie di reato ma basta il tentativo di adescamento. Nel 2022 sono stati registrati 424 casi, il fenomeno è in crescita e il sommerso è assai consistente, complice la colpevolizzazione, la vergogna per essersi fidati di uno sconosciuto. L'età di partenza si aggira attorno ai 9 anni e videogiochi e social network sono i viatici più frequenti. La diffusione del fenomeno segnala l'importanza di condurre attività di educazione ai media nonché all'affettività e alla sessualità.

Per quanto riguarda la prevenzione, molto si può fare. Rizzi si è concentrato sul tema del digital footprint, ossia quante impronte lasciamo quando navighiamo in rete. Attraverso semplici esempi sull'uso delle email o sulle recensioni online ha descritto quante informazioni precise si possano ricavare sulla localizzazione di una persona e sul suo probabile censo, capacità di spesa dedotta da post, stili di vita presunti e altri input di contesto. La triangolazione dei dati disponibili è alla base di queste euristiche. A ciò si aggiungono anche i metadati, ad es. delle foto scattate, che nascondono ulteriori dati preziosi.

Fortunatamente il GDPR protegge i cittadini europei ma le accortezze non sono mai abbastanza. Fra i consigli utili segnalati dagli esperti, oltre ad aver consapevolezza degli account attivi e delle app con accesso a nostri dati che siamo soliti utilizzare quotidianamente attraverso lo smartphone, è importante considerare considerare la Cybersecurity come un insieme di regole di buon senso per mantenere un livello di "igiene digitale" sufficiente. Possiamo monitorare attentamente dove siamo iscritti e a quali servizi diamo accesso ai nostri figli, visualizzare i nostri contenuti come se fossimo altri utenti in modo da capire cosa vedono gli altri, e ancora: separare la email di lavoro da quella personale, adottare l'autenticazione a più fattori, sono alcuni dei modi per farlo.

LINK

https://magazine.fbk.eu/it/news/eserciti-di-bit/

TAG

- #competenze digitali
- #cyberbullismo
- #cybersecurity
- #cybersicurezza
- #fondazioneserics
- #pnrr
- #prevenzione

MEDIA COLLEGATI

- VIDEO registrazione dell'evento: https://www.linkedin.com/video/live/urn:li:ugcPost:7060962220569993216/?actorCompanyId=243693
- Fondazione SERICS (PNRR - cybersecurity) : https://serics.eu/

AUTORI

- Giancarlo Sciascia