Intermediari finanziari e aikido digitale

Lezione V: conosci il tuo nemico (informatico)

Negli articoli precedenti abbiamo spiegato come affrontare i concorrenti, i combattenti e la tecnologia attraverso i principi dell'aikido digitale. Torniamo ora a parlare del concetto di autodifesa. In nessun altro caso l'autodifesa è più utile se non per proteggersi da una nuova forma di offensiva: gli attacchi informatici, la cui frequenza e complessità stanno crescendo in maniera significativa.

Ci concentriamo quindi sugli attacchi informatici e sulla loro crescente frequenza e complessità.
In questo caso è fondamentale «conoscere il proprio nemico». Iniziamo allora a capire se il nemico si trova all'interno o all'esterno dell'azienda. La minaccia proveniente dall'interno è tra le più insidiose da cui difendersi poiché i collaboratori dispongono di ampio e legittimo accesso ai vostri asset e alla vostra infrastruttura. È anche la più difficile da affrontare perché non volete trattare i vostri collaboratori come dei sospetti. Possono esserci vari motivi che fanno sì che un collaboratore si trasformi in un aggressore: errore umano, ignoranza, insoddisfazione circa le opportunità di carriera o l'ambiente di lavoro, e così via. Benché possano essere adottate misure tecniche per limitare il rischio, la più importante e difficile forma di difesa è mantenere una sana cultura aziendale e conoscere le persone che lavorano per noi. Una comunicazione chiara e trasparente è fondamentale.

Gli aggressori esterni hanno altri obiettivi e si suddividono in generale in tre ampie categorie:

1. hacker: non sono mossi da interessi finanziari ma piuttosto dal desiderio di «combattere il sistema» o dal bisogno di gonfiare il proprio ego giocando a Davide e Golia;
2. criminali: cercano solitamente un guadagno finanziario ricorrendo al furto di dati/identità o al ricatto (ad es. tramite Distributed Denial of Service (DDoS) o codifica di dati) o allo spionaggio industriale;
3. terroristi: utilizzano mezzi simili a quelli degli hacker e dei criminali nell'intento di nuocere a Stati, aziende o persone.

Esempi di attacchi
La crescente interconnettività e complessità della nostra infrastruttura globale comporta rischi di vulnerabilità e ha cambiato i vettori di rischio. Di seguito alcuni esempi tipici.

Furto d'identità	Per prima cosa viene violata la password, poi il profilo (ad es. social media) o l'e-mail vengono abusati per distribuire messaggi propri (o virus / trojan) o per ricattare il proprietario. Il phishing ne è un esempio. Nel nostro settore, l'esempio più comune è l'ordine di pagamento fraudolento.
Virus / Trojan	Spaziano dallo spionaggio al tentativo di danneggiare dati e/o infrastrutture su sistemi infettati o di (ab)usare un computer (ad es. botnet).
Furto di dati	Hacking per accedere a un sistema al fine di rubare dati che saranno poi venduti sul mercato nero, utilizzati per nuocere al pubblico o per ottenere un vantaggio dal proprietario. Soprattutto nel settore dei servizi finanziari, il furto dei dati personali dei clienti è un rischio estremamente serio. La situazione finanziaria delle persone rappresenta un'informazione molto sensibile e va assolutamente protetta da abusi criminali.

DDoS	Il Distributed Denial of Service (negazione del servizio) ha lo scopo di far esaurire le risorse di un sistema informatico inviando un enorme quantità di richieste a un determinato server.
Disastro naturale	Interruzione della corrente, incendio, inondazione, terremoto.

Proteggere i dati preziosi – un fattore importante per la fiducia dei clienti
Dobbiamo proteggere i dati dei nostri clienti e dei nostri collaboratori. Dobbiamo anche proteggere i nostri clienti e la nostra attività da eventuali frodi (ad es. pagamenti falsi). E dobbiamo proteggere i nostri sistemi affinché possano rimanere operativi.

Le tecniche da padroneggiare sono talmente ampie che in questo articolo abbiamo deliberatamente deciso di fornire una visione d'insieme. Per tutti questi rischi, la vostra impresa dovrebbe disporre di un chiaro piano di Business Continuity Management (BCM) che consenta di individuare e priorizzare i rischi per poi implementare le misure volte a mitigarli. Tra le misure più comuni vi è quella di avere dei sistemi informatici ridondanti sparsi in varie aree geografiche, postazioni di lavoro di riserva dotate della stessa tecnologia e ulteriori misure procedurali come liste di contatto. Sul sito dell'Associazione Svizzera dei Banchieri (www.swissbanking.org) è disponibile il documento «Raccomandazioni per il Business Continuity Management». Per esperienza sappiamo che è meglio avere un piano, ma ancor meglio è metterlo alla prova. Effettuate un test che simuli un crollo del sistema per vedere se funziona veramente nella pratica e non solo sulla carta.

Domande chiave per il vostro fornitore IT interno o esterno
Per determinare l'efficacia del vostro sistema di difesa potete porre al vostro fornitore IT (interno o esterno) dieci domande chiave:

1. Come vi proteggete da virus, trojan e altri tipi di malware e spam?
2. Avete predisposto firewall e quali sono le regole attive?
3. I vostri sistemi sono protetti da un'autenticazione a due fattori? In caso contrario perché no e quali sono i rischi?
4. Disponete di sistemi di back-up ridondanti e quando è stato concluso con successo l'ultima volta un test di simulazione di crollo del sistema?
5. Disponete di computer in grado di operare in modo indipendente in caso di problemi?
6. Di quali log file disponete e dove sono necessari?
7. Avete definito e implementato una policy «least privilege» per l'accesso ai dati?
8. Avete un inventario dei software in cui sono indicati età, ultimi aggiornamenti e altri dati pertinenti? In caso di software proprietari, sono sempre presenti almeno due persone in grado di decifrare il codice?
9. Quali misure e ulteriori accorgimenti adottate nell'utilizzo di servizi cloud?
10. Quanto è efficace la crittografia dei vostri dati?

Il BCM e la sicurezza informatica non sono questioni da delegare. Dovreste effettuare regolarmente una valutazione dei rischi e coinvolgere i vostri fornitori nel processo. Fate in modo che sia sempre tra le vostre priorità.

Un'ultima cosa: dopo aver pensato a come affrontare i rischi informatici cui potrebbe essere esposta la vostra azienda, pensate a come potete aiutare i vostri clienti a proteggere la loro privacy – soprattutto se i loro figli utilizzano liberamente i social media… tematica che tratteremo nel nostro prossimo articolo sui social media.

Potete inoltre consultare liste di controllo come quelle pubblicate per conto del Dipartimento federale delle finanze e dal team di sicurezza online di UBS.

melani.admin.ch/melani/de/home.html
ubs.com/ch/en/online-services/security.html#tips