Carlo Del Bo, executive advisor della ditta "Gruppo sicurezza" accende un campanello d'allarme

"Occhio, la cybercriminalità è ancora troppo sottovalutata"

Non passa giorno senza che si venga a sapere di violazioni della privacy tramite internet. Se a volte il problema si risolve con un'arrabbiatura, in altre circostanze i grattacapi possono diventare anche molto gravi. Ne abbiamo parlato con un esperto del settore, che ci ha spiegato come la sicurezza personale sia alla base anche di quella di tutta la rete.

Carlo Del Bo

Signor Del Bo, ha l'impressione che, malgrado l'ampia informazione fornita, vi sia ancora una sottovalutazione dei pericoli della cyber criminalità?
Il problema è ancora sottovalutato. Negli anni la presenza dei temi relativi ai pericoli informatici è fortemente aumentato sui media e nel web ma non è sufficiente. C'è ancora ancora molta confusione tra gli utenti e pochi sanno lo scopo della cyber security che è un processo tecnico, organizzativo e culturale che dovrebbe permeare le aziende e i singoli individui.

E quali saranno le conseguenze?
Gli attacchi informatici aumenteranno nel tempo e saranno anche piu' complessi. Per questo motivo ritengo si debba porre maggiore attenzione a questo problema assai complesso.

Secondo una recente ricerca di Kaspersky Lab, solo il 32,9% degli utenti utilizzano soluzioni per la sicurezza. Come commentare questo dato?
Ultimamente ho letto diverse statistiche a riguardo e, ad essere sincero, tutte hanno in comune una percentuale piuttosto bassa di aziende che pianificano appropriate contromisure di cyber security. Molte aziende pensano di non essere cosi importanti o interessanti per un attacco hacker per svariate ragioni.

Si tratta quindi di un mal andazzo abbastanza generalizzato…
È un errore comune che non dovrebbe essere compiuto. Tutti noi possiamo essere oggetti di un attacco hacker per svariate ragioni e con metodi diversi. Tutte le aziende sfruttano la funzionalità della rete a scopi commerciali e usano le diverse tecnologie cloud. Questa metodologia lavorativa determina diverse vulnerabilità che non dovrebbero essere sottovalutate.

Ci sono delle tecniche di violazione della privacy particolarmente subdole, vero?
Alcuni metodi di attacco, per esempio, sono eseguiti da robot hacker che infettano i vari dispositivi mediante attacchi sferrati in automatico non appena rilevano una vulnerabilità indipendentemente dall'azienda oggetto dell'attacco. Una volta infettato un computer, il robot procede at attaccare altri dispositivi senza l'intervento diretto da parte di un criminale informatico.

C'è una "nuova" fascia di utenti che si affaccia al mondo internet e sono gli over 55. È da cercare in queste persone l'anello debole della catena degli utenti?
Non necessariamente la generazione X nata tra il 1961 e il 1980 è sinonimo di insicurezza tecnologica. Ritengo che questa tipologia di persone abbia visto lo sviluppo reale della tecnologia fino a giorni d'oggi e credo sia piu' sensibile proprio perché si è sempre posta un dubbio sull'affidabilità dei piu' moderni e sofisticati sistemi .

Cosa ci dice allora degli altri utenti?
Le generazioni successive ovvero la Y (Millennials) e la Z dei nati dopo il 2000 danno molto piu' per l'elevato grado di sicurezza dei sistemi che molto spesso non è adeguato. Ma indipendentemente dal tipo di generazione, ritengo che tutte debbano essere sensibilizzate e formate riguardo le tematiche dei cyber risks e del loro impatto nel mondo reale. Come è noto, il fattore umano contribuisce ad innalzare o abbassare il livello di sicurezza. Per questo anche noi a Gruppo Sicurezza abbiamo dato vita ad una serie di corsi proprio per ridurre gli effetti umani..

C'è una grossa interconnessione al giorno d'oggi: cosa può fare una ditta come la vostra per proteggere gli utenti? Che mezzi avete a disposizione?
La connessione oggi giorno è quasi assoluta e l'avvento dell'internet delle cose ha contribuito in forma esponenziale all'esplosione della presenza in rete delle aziende. Noi come azienda fondiamo la mitigazione dei rischi cyber su cinque fattore: l'analisi della infrastruttura, l'intelligence, il monitoraggio, le gestione degli incidenti e la formazione.
Ci sono poi dei servizi integrati che facilitano l'analisi dei rischi di cyber security e indirizzano le attività propedeutiche alla revisione dei processi e delle tecnologie informatiche, nel rispetto di quanto richiesto anche delle normative europee.
Inoltre garantiamo un monitoraggio continuo dell'infrastruttura e dei dati del cliente, verificando in tempo reale la situazione hardware e software di tutti i dispositivi utilizzati (pc, server, stampanti...), le vulnerabilità presenti, i tentativi di attacco dall'esterno e l'eventuale presenza in rete (data breach) di informazioni del cliente. Vista la complessità della tematica, cerchiamo di personalizzare la nostra offerta per trovare sempre il miglior rapporto costo-benefici per il cliente.

Si ha l'impressione che gli hacker siano sempre un passo avanti rispetto alle tecniche di difesa: il gap è diminuito negli ultimi tempi?
Direi proprio di no. La dinamicità degli attaccanti è sempre qualche passo avanti. Vengono scoperti centinaia di nuovi malware ogni giorno e molto spesso parte di essi sono realizzati per infettare specifici prodotti o settori industriali. Esiste una specializzazione vera e propria. I clienti spesso contribuiscono ad aumentare il gap tra attaccante e target, non adeguando per tempo i propri sistemi operativi. Questa prassi contribuisce a creare terreno fertile per i nuovi malware che sfruttano le vulnerabilità dei sistemi non ancora aggiornati.

Sette consigli contro la cybercriminalità

- Utilizzate una tecnologia affidabile per la sicurezza informatica e mantenetela aggiornata. Installate, aggiornate e attivate sempre i firewall (che vi proteggono da interventi esterni) e le applicazioni di rilevamento delle intrusioni.
- Utilizzate i browser Web più recenti. Se utilizzate Microsoft Windows attivate la funzione "Aggiornamento automatico"
- Fate attenzione ai siti Web che richiedono l'installazione di programmi. Leggete sempre in modo attentamente i contratti di licenza e annullate il processo di installazione se s'installano programmi aggiuntivi rispetto a quelli desiderati.
- Fornite i vostri dati personali solo sui siti Web che riportano l'icona a forma di lucchetto in fondo al browser o sulla barra degli indirizzi.
- Per mantenere protette le vostre e-mail, utilizzate un prodotto anti-spam. La maggior parte dei software di protezione affidabili per computer sono dotati di questa funzione.
- Fate attenzione ai messaggi e-mail di chi non conoscete, inattesi o anomali. Non aprite gli allegati e non cliccate sui collegamenti contenuti in questi messaggi e-mail.
- Fate attenzione quando ricevete messaggi e-mail che richiedono i dettagli dell'account e non fornite mai informazioni personali alle richieste non sollecitate.

Fonte: www.trendmicro.it

Passiamo alle ditte: quali consigli si sente di dare alle aziende che hanno un grosso tasso di connessione? Limitare l'accesso a dei determinati siti può essere sufficiente? Come ci si dovrebbe comportare nei confronti dei social network, anch'essi pieni di minacce (v. profili fake p.es.)?
Imprenditorialmente non è più possibile limitare la propria presenza in internet salvo rare eccezioni. Penso ogni azienda debba avere un metodo chiaro e sicuro per affrontare le sfide dei rischi da cui posso derivare dei danni anche economicamente molto importanti. Non è piu' possibile improvvisare azioni correttive senza una visione d'insieme delle minacce.

E allora?
I dati sensibili e confidenziali di una azienda sono spesso gestiti da piu' persone e molto spesso vengono duplicati e migrano a terzi per ragioni d'ufficio e operative. Detto questo, è importante far eseguire un'analisi dei rischi mirata all'individuazione dei punti di debolezza, predisporre un piano di contromisure adeguate e aggiornate nel tempo perché le minacce si evolvono e si moltiplicano rapidamente.

Le migrazioni di dati da un sistema all'altro sono momenti molto delicati: per questi processi e più in generale per altre situazioni, quanto è importante rivolgersi a degli specialisti?
Operazioni come la migrazione di un server o l'uso di nuovi sistemi in cloud vanno programmati per tempo sia per la loro efficienza che per la sicurezza. Occorre valutare preventivamente il progetto, capire l'impatto in azienda e formare adeguatamente le persone all'uso corretto del nuovo sistema.
Ritengo si debbano usare sia specialisti che hanno compiti ben diversi e in tandem possono contribuire al successo del progetto.

O.R.