I rischi a cui sono sottoposte le aziende

Le aziende sono a rischio ogni giorno. Virus, hacker e persino errori accidentali degli utenti costituiscono un serio pericolo, con conseguenze altrettanto serie. I casi presentati illustrano questo pericolo attraverso esempi reali di attività dolose e delle loro conseguenze. Tutti questi casi sottolineano l'importanza delle misure preventive, che consentono di minimizzare, se non eliminare, qualsiasi pericolo. Per scoprire come proteggerti, consulta la checklist per la protezione informatica nelle piccole aziende. Per ulteriori informazioni sul funzionamento di Internet e sulle modalità operative degli hacker, leggi l'articolo "L'ABC degli hacker".

Virus

Nell'aprile del 2003, utenti di Internet di tutto il mondo ricevettero da amici e parenti messaggi di posta elettronica contenenti materiale pornografico. Altri si videro negare l'accesso a Internet con l'accusa di aver inviato posta indesiderata. Altri ancora si trovarono iscritti a newsletter che non desideravano. Era chiaro che stava succedendo qualcosa di strano.

Mentre su Internet si susseguivano accuse su accuse, ci si rese conto che il responsabile era un nuovo virus denominato "Klez". Il virus Klez utilizzava diversi trucchi per alimentare la propria diffusione. Prima di tutto faceva credere agli utenti che i messaggi infetti provenissero da persone reali, perché utilizzava gli indirizzi e-mail prelevati dalle agende degli stessi utenti che aveva infettato. Con questo stratagemma sortiva inoltre l'effetto di intasare i sistemi di posta elettronica con una quantità di messaggi di protesta, risposte e recriminazioni del tutto superflui. In secondo luogo, il virus utilizzava oggetti ingannevoli, come ad esempio "Divertentissimo sito Web" oppure "Impossibile recapitare il messaggio", per persuadere gli utenti ad aprire i messaggi infetti.

E, come se non bastasse, nelle sue versioni successive il virus utilizzava i file personali degli utenti come veicolo di infezione. Una volta introdottosi in un computer, Klez ne esaminava il disco rigido, individuava un documento adatto, quindi lo infettava e lo inviava ad altri utenti attraverso la posta elettronica. In molti casi, documenti di carattere privato vennero esposti al pubblico dominio.

Klez sfruttava un problema del programma di posta elettronica Microsoft Outlook che era già stato scoperto e risolto anni prima, attraverso l'installazione di aggiornamenti Microsoft scaricabili gratuitamente. Gli sviluppatori di software antivirus se ne resero conto e aggiornarono i relativi programmi nello spazio di poche ore, eppure il virus imperversò per mesi e mesi. In altre parole, questo virus così aggressivo e distruttivo poteva essere evitato. Klez è stato uno dei virus più distruttivi
del 2003, ma è solo uno delle migliaia di virus che fanno la loro comparsa ogni anno.

Spoofing della posta elettronica e furto d'identità

"Lo ammetto. Sono un appassionato del sito Web eBay. Vi ricorro ormai da anni per mettere in vendita alcuni dei miei articoli più interessanti. Non molto tempo fa ho ricevuto un messaggio del tutto simile a quelli inviati ufficialmente da eBay, con cui venivo avvisato che il servizio nei miei confronti stava per essere sospeso. Ho fatto clic sul collegamento presente nel messaggio e ho aperto quella che sembrava una pagina del sito eBay. Ho inserito le informazioni personali richieste, quindi le ho inviate. Solo dopo mi sono reso conto che c'era qualcosa che non quadrava. Allora ho aperto il sito Web di eBay e ho infine compreso di essere stato ingannato: avevo inviato informazioni di carattere personale a chissà quale fonte sconosciuta".

L'invio di messaggi e-mail che sembrano provenire da altri è un trucco ormai vecchio, conosciuto col nome di spoofing della posta elettronica. Nella maggior parte dei casi, lo spoofing viene utilizzato per indurre l'utente ad aprire un messaggio di posta indesiderata, facendogli credere che provenga da un mittente

legittimo: una pratica sicuramente irritante, ma tutto sommato innocua.

Esiste però un altro tipo di spoofing della posta elettronica, come quello dell'esempio precedente, conosciuto col nome di "phishing", che è sicuramente più dannoso. In genere, un hacker invia un messaggio di posta elettronica che sembra provenire da una fonte ufficiale (ad esempio eBay o Microsoft). Il messaggio contiene collegamenti a un sito Web del tutto simile a quello originale.

Invece, il sito non è che una copertura. Scopo della frode è indurre l'utente a fornire i propri dati personali, a volte per compilare elenchi di utenti a cui inviare posta indesiderata, a volte per trafugare informazioni sull'account utente o persino la sua identità.

Computer rubati

"Ero all'aeroporto e stavo ritirando la mia carta d'imbarco. La custodia del mio notebook era per terra, di fronte a me. Credevo di tenerla sotto controllo, invece non mi sono reso conto di nulla quando me l'hanno rubata". Da un computer rubato si può ricavare fino alla metà del suo prezzo al dettaglio. Non è dunque una sorpresa che migliaia di notebook vengano rubati ogni anno solo negli Stati Uniti.

Il fatto si ripete migliaia di volte all'anno e non basta sostituire il computer rubato per annullarne le conseguenze. La perdita di un notebook, infatti, spesso equivale alla perdita di informazioni cruciali, se non confidenziali.

Nicholas Negroponte, fondatore del Media Lab del MIT (Massachussets Institute of Technology), stava entrando in un edificio protetto quando una guardia gli chiese il valore del notebook che aveva con sé. Negroponte rispose: "Da 1 a 2 milioni di dollari circa". Benché il valore del computer in sé si aggirasse sui duemila dollari, il valore delle informazioni che conteneva era di gran lunga

superiore.

Dato il numero dei computer che vengono rubati ogni anno, è sconcertante vedere quanto pochi siano gli utenti che ricorrono alla crittografia dei dati o fanno uso di password sicure per impedire accessi non autorizzati. E altrettanto sconcertante è il fatto che pochissime piccole aziende istruiscano i propri dipendenti sulle misure di sicurezza di base.

War driving

Il war driving è una nuova forma di pirateria informatica. Bastano un notebook, una scheda di rete non particolarmente costosa, software scaricato gratuitamente da Internet e un'antenna fabbricata con uno di quei tubi in cui vengono confezionate certe marche di patatine per violare le reti wireless private o aziendali, anche da centinaia di metri di distanza.

Gran parte delle reti wireless, infatti, non è assolutamente protetta. Anzi, molti produttori di dispositivi wireless disattivano la crittografia come impostazione predefinita. Gli utenti, poi, tendono a non attivare la crittografia e a non utilizzare altre misure di sicurezza aggiuntive, consentendo a chiunque sia dotato di una configurazione wireless di individuare e sfruttare facilmente la loro connessione. Il war driving è ben più di un innocuo scherzetto: a volte gli intrusi cercano di accedere
ai file e di danneggiare il sistema. Fortunatamente, proteggere una rete wireless è relativamente semplice e la maggioranza dei pirati dediti al war driving può venire scoraggiata attuando poche, semplici procedure.

Informazioni confidenziali

James era dipendente di una nota agenzia pubblicitaria. Avendo riscontrato qualche problema con il computer, contattò il supporto tecnico. Il tecnico arrivò, si

connetté alla rete con un account amministratore e risolvette il problema. Al termine, il tecnico si affrettò ad andarsene per occuparsi del lavoro successivo, ma dimenticò di chiudere la sessione. Preso dalla curiosità, James decise di dare un'occhiata e trovò un foglio di calcolo contenente informazioni sui salari di tutti i suoi colleghi.
E si ripropose di chiedere un considerevole aumento di stipendio.

Fortunatamente per il suo datore di lavoro, James non voleva altro che un aumento. Le cose sarebbero forse andate diversamente se si fosse trattato di un dipendente amareggiato in cerca di vendetta. Ti piacerebbe che i dipendenti conoscessero il tuo stipendio o avessero accesso a tutte le informazioni relative ai salari dell'intera azienda? Quanto potrebbe valere per i tuoi concorrenti questo tipo di informazioni?

La tecnologia può concorrere a prevenire simili inconvenienti, ma non è l'unica risposta. I migliori componenti hardware e software non sono sufficienti se non si dispone anche di politiche, procedure e programmi di formazione validi.

Pirateria informatica

Jill, responsabile di un piccolo sito Web commerciale per la vendita di applicazioni software di nicchia, era molto contenta del nuovo sito, che costituiva un evidente miglioramento rispetto al vecchio. L'azienda poteva ora contare sul proprio server Web e sulla propria connessione a banda larga e non era più costretta a pagare un servizio di hosting del sito. Venerdì sera, Jill andò a casa di buon umore.

Ma il lunedì mattina, al suo ritorno in ufficio, la situazione era completamente cambiata. Durante il fine settimana, infatti, alcuni pirati informatici erano riusciti a violare il sito, eliminandolo, e lo avevano sostituito con materiale pornografico. Inoltre, centinaia di migliaia di persone si erano precipitate a scaricare dal sito immagini su immagini per l'intero fine settimana. L'uso della connessione a banda larga era stratosferico e l'azienda si ritrovava a dover pagare bollette di migliaia

di dollari. Il superiore di Jill aveva già incominciato a ricevere messaggi e-mail di persone che si lamentavano del sito.

All'inizio dell'anno, uno sviluppatore di software antivirus ha sottolineato che i server aziendali ricevono in media 30 attacchi alla settimana. Molti di questi attacchi provengono da pirati informatici con poca esperienza, i quali utilizzano gli strumenti disponibili gratuitamente su Internet per individuare i punti deboli delle reti. Si tratta di strumenti che scandagliano Internet a caso alla ricerca di sistemi vulnerabili e sfruttano tutti i punti deboli che riescono a individuare. Vista l'esistenza di tali strumenti, aziende piccole e poco note sono potenzialmente a rischio quanto le più conosciute multinazionali.

Molti di questi strumenti sfruttano vulnerabilità già note, che possono essere facilmente aggiornate. Per esempio, nel 2001 un gruppo di adolescenti autodefinitosi "Sm0ked Crew" sfruttò una vulnerabilità, già conosciuta e aggiornata da tempo, di un software per server Web per deturpare i siti Web di Intel, Gateway, Disney e del The New York Times. Molto tempo prima che l'attacco si verificasse era già disponibile un aggiornamento per la correzione di quella vulnerabilità, ma molti amministratori non l'avevano installato. Sarebbe bastato prendere le dovute precauzioni e, in particolare, utilizzare un software aggiornato per prevenire l'attacco.

Se le aziende per prime non prendono le misure di sicurezza più elementari per proteggersi da adolescenti armati di strumenti largamente disponibili, come possono sperare di difendersi da attacker esperti e competenti, animati da intenzioni criminose?

Backup dei dati

Kevin era l'amministratore delegato di uno studio di architettura in espansione. Lo studio contava 30 dipendenti e un buon numero di clienti in diverse parti del mondo, per cui si affidava alla posta elettronica per mantenere i contatti. In

particolare, i dipendenti utilizzavano la posta elettronica per tenere traccia delle richieste di modifica inviate dai clienti. La posta elettronica costituiva perciò un elemento assai importante dell'attività aziendale. Un giorno il server della posta elettronica fu soggetto a un errore hardware irreversibile, che causò il danneggiamento dei dati.

"Non c'è problema", pensò Kevin, "il supporto tecnico ha un backup dei dati, per cui lo utilizzeremo per ripristinare il sistema". L'azienda disponeva infatti di un'elaborata libreria nastri e aveva diligentemente duplicato i backup di importanza vitale, che conservava separatamente. Solo dopo un'intera giornata passata a cercare di ripristinare il sistema di posta elettronica dai nastri di backup, si resero conto che il backup non era stato eseguito correttamente. Non si erano mai accorti del problema e non avevano mai verificato che il ripristino dei dati funzionasse correttamente. Inoltre, non disponevano di alcun piano di ripristino d'emergenza.

La protezione delle informazioni non significa semplicemente dotarsi dei componenti hardware e software più adeguati, ma consiste anche nel seguire procedure adeguate e nel concentrare le risorse nei sistemi di vitale importanza per l'azienda.

SecureTech nace da un progetto per essere il security partner delle aziende, la vostra sicurezza è la nostra miglior garanzia per un lavoro in espansione ed un businees nuovo che fa crescere la vostra azienda.

Lavoriamo in sicurezza per mettere al sicuro il Vostro futuro, per noi mettere al sicuro i Vostri dati significa mettere al sicuro il Vostro lavoro, rendere sicuri i Vostri dati significa garantire il Vostro futuro, la Vostra AZIENDA.

Loris Calipari