PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 7 - numero 1310 di giovedì 01 settembre 2005

ALLARME DEGLI ESPERTI SUI RISCHI DI ATTACCHI INFORMATICI

Spaventano i "virus dormienti"

Gli esperti della ANSSAIF (Associazione Nazionale Specialisti Sicurezza in Aziende di Intermediazione Finanziaria) stanno seguendo con attenzione e preoccupazione

l'evoluzione dei virus informatici, sia nella tipologia che nell'andamento degli attacchi.

Ci riferiamo, ad esempio, ai "virus dormienti", alle centinaia di varianti di una stessa tipologia, ad un trend di diffusione in crescita, ecc.

La paura degli esperti è che si stia preparando un attacco in "grande stile", finalizzato o a mettere in crisi il sistema finanziario occidentale, oppure a rendere ancora più gravi le conseguenze di un attacco terroristico perpetrato con esplosivi o sostanze bio-chimiche; possiamo citare, ad esempio, azioni tese a rendere assai difficoltosi gli interventi di soccorso e di ripristino, quali: eccesso di traffico sulle reti telematiche, blocco dei cellulari per un lungo periodo, oscuramento dei server dedicati al controllo aereo o alla Protezione Civile, ecc..

Pensiamo al sistema di regolamento fra banche: un attacco terroristico disastroso, ad alto impatto anche emotivo, seguito dal blocco delle comunicazioni e dei sistemi informativi degli intermediari finanziari, se prolungato nel tempo, data la gravità, può avere un effetto drammatico se non ci si è preparati in anticipo.

L'enfasi deve essere sempre orientata al rafforzamento delle difese ed alla predisposizione di opportune misure preventive; pertanto, anche in questo caso, in un'ottica di approccio che tende sempre ad essere pro-attivo, riassumiamo quelle che potrebbero essere delle azioni da intraprendere, sia in un'ottica a brevissimo termine, sia nel lungo periodo; comunque, la tipologia di evento sopra descritta va, a nostro parere, analizzata e simulata a tavolino quanto prima (tra l'altro, rientra pienamente negli scenari descritti da Banca d'Italia nelle sue linee guida del luglio 2004).

Alcune contromisure, da noi riportate qui di seguito, appariranno "vecchie", ma abbiamo ritenuto opportuno ripeterle, in quanto non ci risulta che siano molti gli intermediari che le abbiano introdotte.

L'ANALISI DEI FATTI

Proviamo innanzitutto a sintetizzare le motivazioni alla base di questa crescente preoccupazione.

Iniziamo con il riflettere su alcuni fatti.

- In passato abbiamo assistito a feroci attacchi di alcuni virus (Red code; nimda; gaobot; ecc. per citarne alcuni) che hanno colpito praticamente tutte le aziende a livello mondiale;

- c'è stato poi un calo sia in frequenza di attacchi sia nella severità (19 alert nel 2002; 16 nel 2003); ciò malgrado non fossero migliorate di molto le difese (cfr. indagini: CSI/FBI, Australian High Tech Crime Centre; ecc.);

- anche gli attacchi terroristici erano diminuiti in gravità e frequenza;

- si è poi avuto un incremento nel 2004 e negli ultimi 18 mesi si sono avuti molti più allarmi virus - a parità di gravità - che nei due anni precedenti sommati;

- ma ciò che preoccupa di più, è che si sta assistendo ad un incremento nelle varianti di alcuni worm (ad esempio: ci sono oltre 300 varianti di NETSKY e BAGLE, worms di tipo memory resident; un centinaio di varianti di MYTOB; ecc.), quasi ad indicare un tentativo di sperimentare tutte le possibilità sia su come ingannare l'utente sia sulle finalità (NETSKY e BAGLE, ad esempio, hanno avuto mutamenti nell'oggetto, nel messaggio, negli allegati, ecc.);

- ci sono worm che ingannano il ricevente un messaggio affinché apra un messaggio o si rechi su un certo sito, ed altri che invece sfruttano i "buchi" del sistema operativo del computer;

- riemergono vecchi virus (ad esempio: SOBER, GAOBOT, ecc.) con nuove varianti;

- ci sono virus in "appoggio" all'azione di altri (ad esempio: WURMARK e BOBAX);

- ci sono trojans che cercano file di EXCEL, WINWORD o HTML e li spediscono all'esterno;

- ci sono trojan che incriptano questi file e li lasciano sull'hard disk dove li hanno letti (ad esempio, a fini di ricatto);

- ci sono dei worm che hanno avuto l'unico scopo di entrare nei computer per cancellare precedenti versioni, forse in previsione di una nuova versione che sarebbe probabilmente andata in conflitto (se no, perché?);

- ci sono virus il cui unico scopo è quello di ottenere informazioni sul possessore: nome, cognome, indirizzo, uso del computer, password, abbonamenti, gusti, ecc.; molti a fini commerciali, tanti ai fini di furto d'identità;

- sappiamo, altresì, che non possiamo escludere, per esperienza, che i virus siano utilizzati o creati anche da terroristi;

- e così via: potremmo proseguire ancora, ma riteniamo sufficienti le informazioni elencate, per i nostri fini.

Possono sorgere, alla luce di quanto sopra, domande quali:

- le molteplici varianti di uno stesso worm o trojan sono state create esclusivamente per migliorare l'attacco, oppure nascondono un preparativo per "qualcosa" di grosso, di serio?

- I migliaia di trojan che hanno infettato milioni e milioni di computer (oltre 12 milioni l'anno scorso) cosa hanno raccolto? Quali notizie? (da notare che i Paesi più colpiti sono stati quelli dell'Europa Occidentale e gli USA)

- Le informazioni ottenute dagli hacker a cosa sono servite? Molte informazioni sono state chiaramente utilizzate per ricatto, ripicca, furto, ecc. Sono state utilizzate tutte?

- Ci sono delle informazioni "congelate" da qualche parte? Se sì, per farci cosa?

- Possiamo escludere che degli hacker abbiano raccolto le password degli amministratori dei server e possano quindi prenderne il possesso in qualsiasi momento?

Aggiungiamo qualche altra informazione più recente.

Da qualche tempo a questa parte è aumentato il numero dei sistemi operativi i cui "buchi" possono essere sfruttati da nuovi virus: parliamo di sistemi SAP, CISCO, piuttosto che EPOC o SYMBIAN (telefoni cellulari). I mainframe sono fino ad oggi rimasti immuni: perché? Non hanno il TCP/IP a bordo? (o lo sono già stati e non ce ne siamo accorti?). In aggiunta, nei computer si trovano dei virus la cui "firma" o tipologia è sconosciuta: trattasi di virus "dormienti"? In attesa di cosa?

A questo punto possiamo trarre queste conclusioni:

- vi è una crescente sperimentazione di nuovi worm e trojan;

- si riscontrano virus dormienti;

- le informazioni nel frattempo raccolte dai vari trojans forse non sono state totalmente sfruttate;

- vi è un incremento notevole nel numero e tipologia di sistemi che possono essere violati;

- le contromisure adottate dalle aziende rispettano senz'altro i requisiti "minimi" richiesti, ma nella maggior parte dei casi non sono ancora aggiornate in base alla recrudescenza del crimine.

Possiamo allora, alla luce di quanto sopra, escludere che qualcuno, chissà dove, stia preparando un attacco, non solo sui computer di casa, ma contemporaneamente sulle reti di computer, cliente e server, firewall e routers di un'azienda?

Perché? Ci possono essere tanti perché. Perché l'azienda è un intermediario finanziario, oppure perché collabora con una Nazione presa di mira, oppure perché è inglese, o spagnola, o italiana.

Chiaramente non abbiamo la risposta. Ma qualcosa dobbiamo fare. Nessuno di noi si può scordare la giornata in cui Red Code ha colpito le aziende in tutto il mondo. Forse oggi siamo tutti più pronti, ma per un attacco "tradizionale". Se i programmi virali giacciono nelle nostre reti, già la situazione è diversa.

Se l'attacco è contemporaneo su tutti i computer dell'azienda, abbiamo una situazione ancora più grave.

LE POSSIBILI SOLUZIONI

Cosa fare?

Elenchiamo qui di seguito quello che l'esperienza suggerisce.

Approccio orientato prevalentemente alla prevenzione e graduato nel tempo, in modo da essere ragionevolmente certi di

ottenere risultati concreti:

- nel brevissimo termine (contromisure tecniche e procedure per la gestione della continuità in caso di emergenza);

- nel medio (ad es: incremento nella quantità e qualità dei controlli; modifiche organizzative);

- nel lungo (ad es: creazione in azienda di una cultura della sicurezza in termini di qualità del servizio e prevenzione da incidenti).

Operare gli interventi nel breve-medio suddividendo l'approccio in due aree distinte:

- le infrastrutture,

- gli utilizzatori.

Dedicare due team distinti (a pensare, progettare, realizzare i controlli e l'"hardening"; ecc.) per le due aree indicate; in particolare, non trascurare affatto la possibilità di affidare in toto l'hardening delle infrastrutture a terze parti specializzate, concentrando il personale interno sugli aspetti ove è maggiormente richiesta la conoscenza dei processi aziendali, maggiore riservatezza, ecc.

Eseguire attività quali:

- Individuare Virus "non firmati", non riconosciuti fra quelli noti (possono nascondere sw ad hoc per catturare informazioni);

- Non limitare la sorveglianza sui sistemi di sicurezza perimetrale ed interna al solo orario d'ufficio;

- Individuare attività anomale di eccesso di traffico su una lan;

- Indurre gli amministratori dei server a cambiare la password, almeno una volta al mese, controllando non sia la stessa ripetuta ogni due mesi!;

- O meglio ancora, dotare gli amministratori di sicurezza di "one time password", nonchè valutare con attenzione la possibilità di introdurre sistemi biometrici di controllo accessi;

- Non rimandare dei controlli, su eventi anomali, al giorno dopo;

- Controllare minuziosamente l'elenco delle macchine in rete, senza escludere nessuna lan (ad esempio: quelle degli "architetti" o di test);

- Cercare di evitare di avere database con dati riservati o peggio sensibili direttamente collegati ad internet;

- Individuare Attività anomale del pc, ad esempio, segnalando accessi fuori orario;

- Sviluppo software: disegno include la sicurezza;

- Cultura di sicurezza agli sviluppatori di software;

- Disseminare, in generale, una cultura della sicurezza in azienda, verificandola periodicamente;

- Inserire i controlli sulla compliance alle esigenze di sicurezza e business continuity nei processi di disegno e realizzazione di

nuovi sistemi;

- Sensibilizzare gli utenti - interni ed esterni - alle tematiche di protezione dei dati, continuità del business, qualità del servizio;

- Eseguire almeno annualmente una analisi del rischio ICT (in modo "serio", non in via simbolica., come avviene in molte aziende);

- Integrare le esperienze, conoscenze, attività, dei colleghi impegnati nell' ORM (Operational Risk Management), sicurezza fisica ed ICT, Business Continuity, auditing, usando come "collante" l'Organizzazione e le Risorse Umane, in modo da facilitare sia la comprensione dei fatti individuati sia la individuazione delle possibili soluzioni;

- Ipotizzare l'assenza dei sistemi informativi a sostegno dei processi di regolamento e compensazione e, pertanto, redigere, e sperimentare, gli opportuni piani di gestione dell'emergenza.

(Fonte: CLUSIT; ANSSAIF - Associazione Nazionale Specialisti Sicurezza in Aziende di Intermediazione Finanziaria. www.anssaif.it)

---

www.puntosicuro.it