DOCUMENTO SULLA SICUREZZA INFORMATICA INDUSTRIALE

POLIZIA DI STATO
Polizia Postale e delle Comunicazioni
Compartimento per l'Emilia-Romagna

UNINDUSTRIA BOLOGNA

DOCUMENTO SULLA SICUREZZA INFORMATICA INDUSTRIALE

1. Quali tipi di aziende possono essere colpite da attacchi informatici? Con quali scopi? Con quali tipi di attacco?

Tutte le aziende sono vittime potenziali. Restringendo l'assioma secondo cui l'unico PC sicuro è quello spento, si può sostenere che **l'unico PC sicuro è quello che non è mai stato acceso**. Ovviamente il rischio aumenta in proporzione al patrimonio aziendale e alla delicatezza delle informazioni custodite.

Gli attacchi variano in base all'obiettivo che vuole essere raggiunto. L'hacker può limitarsi a "semplici" interruzioni di servizio (DOS, *Denial Of Service*) per scopi dimostrativi o di ritorsione, oppure puntare alla compromissione dei dati seguiti da estorsione dietro la minaccia di non riparare il danno inflitto, fino ad arrivare al furto di dati sensibili per fini industriali/commerciali.

Rispetto a qualche anno fa, quando gli attacchi venivano per la maggior parte eseguiti mediante scansioni ad ampio raggio alla ricerca di possibili falle nella sicurezza, oggi gli obiettivi vengono maggiormente studiati a tavolino, in modo da massimizzare l'impegno dedicato rispetto al guadagno.

Quindi importante porre particolare attenzione a tutti i tipi di informazione che vengono resi pubblici dall'azienda - quando possibile - e che riguardano il loro stato di salute economica oppure il possesso di informazioni preziose, (progetti, brevetti, prototipi, ecc.), poiché queste possono renderla maggiormente appetibile agli occhi dei criminali informatici.

E' importante comprendere che le falle della sicurezza non sono solo quelle digitali ma comprendono anche tecniche di tipo sociale mirate all'acquisizione di informazioni. Telefonate di finti operatori, password scritte su foglietti, stampe di informazioni sensibili cestinate sono solo alcuni esempi di possibili aiuti forniti involontariamente.

Le moderne tecniche di cyber/social-attacco possono essere rivolte a tutte le imprese, indipendentemente dalla dimensione e dal "peso" economico, e si può tranquillamente asserire che nessuno è al sicuro.

2. Gli obiettivi sensibili a cui sono rivolti gli attacchi:

2.1 *Home Banking*

Il conto corrente online è molto utilizzato dalle aziende vista la facilità di utilizzo e i bassi costi di gestione rispetto alle modalità tradizionali. Questo lo rende anche uno degli obiettivi di maggior valore per i pirati informatici, nonostante le procedure di sicurezza adottate da tutti i circuiti bancari.

2.2 Posta elettronica

La diffusione esponenziale della posta elettronica negli ultimi anni ne ha fatto uno dei maggiori canali di informazione per la pirateria informatica, come fonte di acquisizione di dati sensibili utilizzati poi per perpetrare il vero e proprio crimine informatico.

2.3 Dati digitali (anagrafiche, progetti, gestionali, ecc.)

Vero e proprio patrimonio spesso sottovalutato, il dato digitale in tutte le sue forme rappresenta una delle mete più ambite per il pirata informatico. Sotto forma di anagrafica può essere utilizzato come elenco di email da utilizzare per lo spamming/phishing; come gestionale può contenere informazioni sullo stato economico dell'azienda e sulle transazioni con i fornitori; come archivio documentale può contenere disegni, progetti, documenti e altre proprietà intellettuali preziosissime per l'azienda.

2.4 *Web server* non *in hosting*

Con l'aumentare delle prestazioni sia di banda internet che di hardware a disposizione delle aziende, è diventato abbastanza comune integrare internamente il proprio sito web istituzionale, senza quindi appoggiarsi a provider esterni per la gestione dello stesso.
Questo porta alla necessaria apertura di "porte" pubbliche su internet, rendendo potenzialmente ancora più semplice l'intrusione di male intenzionati anche sulla rete interna.

3. Tipologie di attacchi più comuni a cui può essere sottoposta un'azienda:

3.1 *Phishing*

Il *phishing* è un tipo di frode informatica volta a sottrarre identità digitali appropriandosi di informazioni personali e riservate, prevalentemente nome utente e parola chiave (*user* e *password*).
I settori maggiormente colpiti dalle attività di *phishing* sono l'*home banking* ed i profili *on line* delle carte di credito, senza però trascurare anche varie tipologie di *account*, come e-mail, conti gioco *on line*, profili *Ebay*, e altri.
Il maggiore strumento di diffusione del *phishing* è la posta elettronica.

Classico esempio la ricezione di una mail apparentemente proveniente dal proprio istituto di credito in cui è presente un link che reindirizza ad un sito internet la cui grafica rispecchia, più o meno fedelmente, il layout originale della propria banca; l'utente viene quindi invitato ad inserire le proprie informazioni personali (inclusa la eventuale *OTP-One Time Password*) adducendo fittizie motivazioni, quali ad esempio l'aggiornamento o la conferma degli stessi dati per motivi di sicurezza bancaria.

Se l'utente, in buona fede, aderisce alla richiesta ne consegue che le sue credenziali utili per l'accesso ai servizi di home banking vengono catturate da soggetti non autorizzati. Molto diffusi, soprattutto negli ultimi anni, anche i virus informatici che, una volta infettata la macchina dell'utente, trasmettono telematicamente i dati a terze persone male intenzionate.

Una volta in possesso delle credenziali dell'utente, il phisher è in grado di accedere al sistema home banking compromesso e quindi effettuare disposizioni di bonifici.

Bisogna tener conto che vengono prese di mira anche le piattaforme gestionali che le aziende utilizzano per la compilazione degli ordinativi di pagamento; il phisher, che in questo caso non agisce direttamente sul conto corrente, si limita a redigere dei falsi ordinativi di pagamento confidando che, una volta caricati nel sistema, sfuggano alla successiva verifica da parte del personale incaricato ad eseguire materialmente i bonifici bancari. Le aziende più a rischio, non dal punto di vista informatico ma per quanto attiene le attività di controllo, sono quelle che quotidianamente eseguono molteplici pagamenti on line essendo più probabile che un falso ordinativo passi inosservato.

3.2 *Man In The Middle*

Man in the middle attack, letteralmente l'attacco dell'uomo in mezzo, conosciuto anche con gli acronimi MITM o MIM, è un tipo di attacco informatico con cui un soggetto non autorizzato, in gergo "attaccante", riesce a intromettersi nelle comunicazioni tra due parti con una modalità tale che nessuna di esse si accorga della compromissione del collegamento che le unisce reciprocamente, ma soprattutto con la possibilità di leggere i contenuti dei messaggi nonché di inserirne o modificarne a piacere, senza che nessuna delle due parti si renda conto dell'intromissione.

L'attacco si considera completato quando l'intruso è in grado di osservare, intercettare e replicare verso la destinazione prestabilita il transito dei messaggi tra le due vittime, ottenendo il controllo completo di quelle comunicazioni.

Sono evidenti le possibili conseguenze che un attacco *Man in the middle* può determinare nel caso di comunicazioni tra aziende; ad esempio tra cliente e fornitore l'attaccante potrà disporre ordinativi, pagamenti, mutare le coordinate bancarie, ecc.

Per estensione, il termine *Man in the middle*, anche se impropriamente, viene utilizzato anche per indicare situazioni in cui l'attaccante, senza effettuare un assalto informatico come quello sopra descritto, arriva comunque, tramite altri artifizi, a sostituirsi, più o meno integralmente ad almeno una delle due parti che stanno comunicando tra loro,

oppure riesce a presentarsi illecitamente a terzi in nome, nel caso di specie, di un'ignara azienda.

Il criminale prima carpisce informazioni sulle aziende attraverso la rete internet, utilizzando le informazioni di insiders aziendali, violando indirizzi e-mail, accedendo a *devices* aziendali smarriti o rubati, ecc., ma anche tramite visure camerali o interrogazioni presso imprese che forniscono consulenze aziendali o informazioni creditizie. Successivamente, spesso anche approfittando di diversi fattori contingenti quali giorni di chiusura, diverso fuso orario, ubicazione territoriale, lingue straniere che rendono difficoltosi sia i contatti in tempo reale come quelli telefonici (le aziende cinesi, ad esempio, si relazionano molto spesso con quelle italiane a mezzo email) sia eventuali forme di verifica o controllo, l'attaccante si sostituisce all'azienda x e si presenta alla ditta y. Effettua poi ordinativi fraudolenti o finge di effettuare forniture attraverso pagamenti anticipati, oppure, nel caso di aziende con pregressi rapporti commerciali, comunica nuove coordinate bancarie per la ricezione di pagamenti di precedenti commesse ancora insolute.

Le false comunicazioni sono realizzate anche avvalendosi di indirizzi email appositamente creati che ricordano direttamente quelli dell'azienda presa di mira. (Esempio: se l'indirizzo reale della società XYZ S.p.A. è info@societaXYZ.com, il criminale creerà l'indirizzo societaXYZ@gmail.com, oppure, se l'indirizzo del direttore commerciale è antonio.rossi@societaXYZ.com, verrà creato antonio.rossi@yahoo.com).

È bene evidenziare che la prima email di comunicazione del cambio dei recapiti aziendali con quelli utilizzati per la frode avviene spesso proprio attraverso l'indirizzo email reale dell'azienda violata, che viene utilizzato una tantum dal reo per rendere più credibile la truffa.

3.3 Criptazione dati digitali

In genere questo attacco colpisce sistemi operativi Windows Server, gestibili da remoto attraverso il protocollo Remote Desktop (porta TCP 3389). Gli hacker si introducono nel sistema target con le credenziali di accesso (*UserId* e *Password*) dell'amministratore di rete, che nella maggior parte dei casi hanno bassa complessità (per esempio UserId = "admin" e Password = "password"). Una volta ottenuto il controllo della macchina, l'hacker installa un eseguibile (detto "*Cryptolocker*") per criptare i file con estensione più comune (.txt, .doc, .xls, .pdf, .mdb, ecc), lasciando come firma un file di testo con le istruzioni che la vittima deve seguire per recuperare i file originali. Tale file è impostato per aprirsi ad ogni avvio del sistema operativo.

Si ipotizza che gli hacker utilizzino un programma di *port scanning* per individuare nella rete quali siano i sistemi vulnerabili (server Microsoft Windows dietro un *firewall* con porta TCP 3389 aperta) e poi tentino un attacco "*brute force*" per violare le *password*. Attacco che per sistemi con password poco complesse ha un'alta percentuale di successo e richiede breve tempo per essere portato a termine.

Spesso e volentieri gli hacker operano nella rete raggiungendo il bersaglio dopo aver at-

traversato una catena di *proxy* (rete TOR o similare) che modifica l'indirizzo IP sorgente, per cui i messaggi risultano come essere inviati all'ultimo nodo della catena (exit node) e non dal mittente originario.

Questi server *proxy* possono essere stati creati ad hoc o essere stati "bucati" da precedenti attacchi (in gergo diventano *zombie* di una *botnet*) per cui non vi è possibilità di risalire la catena fino al reale mittente attraverso l'analisi dei file di log.

Anche i server mail da cui sono state inviate le richieste estorsive rientrano nel circuito sopra descritto, per cui risulta praticamente impossibile rintracciare gli autori della condotta illecita se non attraverso tecniche di intercettazione attiva.

4. Prevenzione (contromisure)

Pur osservando che non esiste una strategia unica per l'operatore della sicurezza informatica, in ogni azienda ci si dovrebbe attenere ad alcune linee guida fondamentali. Occorre comunque ricordare che quando si parla di sicurezza informatica si deve fornire sempre un riferimento temporale. Infatti, **una rete è sicura in un tempo limitato.**

a) Implementazione di un sistema IPS/IDS

Gli attacchi dall'esterno possono essere prevenuti (*Intrusion Prevention System*) mediante l'utilizzo di firewall perimetrali software o hardware, e rilevati attraverso software appositi (*Intrusion Detection System*) oggi ormai integrati nella maggior parte degli stessi firewall.

b) Utilizzo di software antivirus

Gli antivirus dovrebbero essere utilizzati su tutti i server e su tutti i client e mantenuti costantemente aggiornati. L'utilizzo di antivirus datati non consente la rilevazione delle ultime definizioni dei virus e dunque ne rende impossibile la conseguente rimozione.

c) Separazione dei servizi

Con il diffondersi delle tecnologie di virtualizzazione è possibile implementare più macchine virtuali sulla stessa macchina fisica.

Ciò consente la separazione dei servizi con un conseguente risparmio dei costi e aumento della sicurezza. In particolare, è opportuno realizzare una macchina dedicata per il database degli utenti (che non deve essere in alcun modo raggiungibile dall'esterno) e l'implementazione di un proxy server per il controllo degli accessi a Internet.

d) Limitazione dei servizi attivi

E' inutile attivare servizi che poi non verranno utilizzati (ad esempio l'ftp per il trasferimento dei file) o pubblicare servizi che hanno rilevanza esclusivamente interna. Si suggerisce di negare di default l'accesso dall'esterno a tutti i servizi, per poi aprire di volta in volta solo quelli strettamente necessari agendo sulle regole del firewall.

e) Gestione attenta delle policy di gruppo

Gli utenti che accedono alle risorse della rete dovrebbero essere divisi in gruppi a ciascuno dei quali l'amministratore di rete concederà privilegi differenti. Ad esempio, l'utente di norma non dovrà essere in grado di installare applicazioni sulla propria macchina, mentre l'ospite (guest) potrà vedere solo le cartelle pubbliche ma non dovrà avere una propria home sul file server.
Allo stesso modo si separeranno i livelli di amministrazione, definendo ad esempio gruppi come il Local Administrator (amministratore della macchina locale), l'*Administrator* del *Domain Controller* e il *Domain Administrator* (amministratore del Dominio). I ruoli possono poi ruotare in modo da consentire a ciascun operatore di avere una conoscenza della rete a 360° (job rotation).

f) Sicurezza delle password

La sicurezza delle password per accedere ai servizi di dominio passa attraverso un sistema di cifratura simmetrica realizzato attraverso appositi algoritmi di hash. La politica delle password prevede di stabilire dei requisiti di lunghezza e complessità. Le best practices implicano:

- lunghezza minima 10 caratteri;
- combinazione di caratteri alfanumerici maiuscoli e minuscoli e caratteri speciali;
- scadenza periodica delle password (per esempio ogni 6 mesi);
- vincolo di variazione di almeno il 70% dei caratteri tra la vecchia e la nuova password;
- blocco dell'account utente per almeno 30 minuti dopo 3 tentativi di login errati;
- scelta di password che non contengano in toto o in parte il nome e cognome dell'utente;
- responsabilizzazione del dipendente sulla custodia della password personale.

g) *Security through obscurity*

La complessità della rete aumenta la sicurezza. Ciò incentiva l'utilizzo di sottoreti e VLAN all'interno della stessa rete.

h) Gestione da remoto attraverso VPN

L'accesso da remoto attraverso la rete Internet può essere implementato attraverso vari protocolli. Si sconsiglia l'uso del protocollo RDP o programmi client-server in cui l'autenticazione avviene solo tramite User ID e password. L'accesso via VPN con IPsec con certificati o OpenVPN è da privilegiare. I certificati per l'accesso vanno consegnati manualmente su chiavetta USB a ciascun dipendente autorizzato. Si consiglia in ogni caso di limitare l'accesso via VPN solo per scopi amministrativi.

i) *Layered security*

La sicurezza andrebbe implementata ad ogni livello di rete (riferendosi alla pila ISO/OSI). L'uso del doppio firewall per creare una zona "demilitarizzata" DMZ è opportuno se si utilizza un web server, in modo da separare la Intranet aziendale dalla rete Internet.

I) ***Diversity of defense***

Diceva Sun Tzu ne "L'arte della guerra": 'Conoscendo gli altri saprai attaccarli. Conoscendo te stesso, saprai difenderti'. E allora mischiando le carte si può essere inattaccabili: sfruttando tecnologie diverse (per esempio un dominio con macchine Windows e Linux integrate), utilizzando hardware di marche diverse e affidandosi a software di produttori diversi si abbassa il rischio che un potenziale hacker/cracker sia così "skilled" da conoscere ogni vulnerabilità della rete.

A cura di:

Dir. Tec. Princ. Ing. Francesco TAVERNA
Ispettore Capo Luca VILLANI
Sovrintendente Capo Franco GRILLI
della Polizia Postale e delle Comunicazioni - Compartimento per l'Emilia-Romagna

Uffici Comunicazione e Organizzazione di Unindustria Bologna

Con il contributo del dott. Salvatore COSTANZO (COGEFRIN S.p.A. - Bologna)