OpenDoc

Is time to rethink security concept!

A great cyber security and development company

Sicurezza di un’organizzazione: da dove parto?

Talvolta le organizzazioni che vogliono mettere in sicurezza la propria infrastruttura sono in difficoltà nel capire da dove partire. Ho cercato di riassumere alcuni concetti base, sperando che questo possa tornarvi utile o quanto meno possa darvi un'idea generale del lavoro che vi aspetta.

Inventario delle risorse

Per prima cosa è importante essere a conoscenza di quali risorse abbiamo, in modo da poterle proteggere adeguatamente. Sembra un'attività banale, ma non lo è, soprattutto in aziende che non hanno al proprio interno risorse umane adeguatamente skillate. Dobbiamo sapere esattamente quali informazioni abbiamo e dove esse risiedono. Inoltre dobbiamo dividere la varie informazioni in diverse categorie in base all'importanza che esse rivestono all'interno della nostra organizzazione.

Alcuni esempi di risorse sulle quali effettuare l'inventario: locali, pc, server, dispositivi mobili, software, filesystem. Per ogni risorsa dovremo avere a disposizione ulteriori informazioni che possono esserci utili in caso di problemi di tipo logistica/hardware/software, quindi: data di acquisto, validità garanzia, codice seriale, contatto e contratto di assistenza, eventuale link con cliente/fornitore,…

Disponibilità delle informazioni

Qualsiasi sia lo scopo della nostra organizzazione, dobbiamo assicurarci di avere a disposizione tutte le informazioni che potranno aiutarci a monitorare la situazione in tema di information security. È perciò importante implementare un syslog server (o più di uno) verso il quale inoltrare i log dei quali abbiamo bisogno. Allo stesso scopo è importante, quando si acquista un nuovo device, verificare che questo abbia la possibilità di generare ed inviare log via syslog o snmp trap.

Applicare le patch

Un piano di applicazione delle patch rilasciate dai vendor è fondamentale per mantenere la propria infrastruttura ad un livello di sicurezza ragionevole. Al di la di quanto gli host/servizi da aggiornare siano critici ed importanti per il proprio business, le patch devono essere applicate. Stabiliamo un giorno della settimana o un giorno ogni due settimane nel quale sappiamo che dobbiamo dedicarci all'applicazione delle patch. È opportuno fissare delle finestre di manutenzione adeguate e che permettano di avere del tempo a disposizione per effettuare gli aggiornamenti in tutta tranquillità. Non sottovalutiamo le note di release e leggiamole con attenzione, in quanto talvolta possono contenere delle informazioni assolutamente vitali. E' importante inoltre avere sempre un piano B a disposizione o una funzionalità di rollback, spesso messa a disposizione dai vendor stessi.

Le patch sono fondamentali per mantenere i nostri device e le nostre applicazioni efficienti. Non sottovalutiamo inoltre il fatto che i vendor talvolta legano la possibilità di darci supporto in caso di problemi proprio al fatto di avere una versione sufficientemente aggiornata del software in questione.

Cambiare le password di default

Vale per tutto: server, router, applicazioni, dispositivi IoT,… In ogni momento gli attaccanti eseguono script che tentano di effettuare l'autenticazione utilizzando le credenziali di default dei vari dispositivi. Ogni host (nessuno escluso) collegato in rete e raggiungibile pubblicamente è potenziale vittima di questo genere di attacco.

Segmentare la network

E' fondamentale segmentare correttamente la rete. La segmentazione base e più banale può avvenire a livello di firewall, configurando diverse network per le diverse connettività gestite (lan, wan, dmz, test,…). E' inoltre preferibile aggiungere ulteriore segmentazione a livello di switch, utilizzando dispositivi che supportino le vlan e permettendo così una corretta separazione dei vari domini di broadcast. Questo, oltre a rendere più ordinato e funzionale il traffico presente nella nostra infrastruttura, aggiunge un livello di sicurezza in più, rendendo il compito più arduo ad eventuali attaccanti.

Segmentare il livello applicativo

Una corretta segmentazione a livello applicativo, al pari di quella a livello networking, rende la nostra infrastruttura più sicura. E' perciò preferibile separare la parte di accesso all'applicazione (frontend) da quella dove sono effettivamente presenti i dati (backend). Frontend e backend dovrebbero essere hostati su macchine diverse, preferibilmente su network diverse. Poniamo l'esempio di un'applicazione che fornisce funzionalità di remote banking: in questo caso la parte di frontend risiederà sulla dmz, mentre la parte di backend risiederà in lan (o in una diversa network ad hoc).

Segmentare il livello di gestione (management)

L'accesso alle console di amministrazione dei vari dispositivi critici (switch, router, firewall, ipmi) dovrebbe essere riservato agli amministratori di sistema. E' quindi opportuno configurare una network ad hoc nella quale rendere attive le varie console amministrative e proteggere l'accesso a questa network attraverso opportune acl.

Disabilitare ciò che non è necessario

Se una cosa non ci serve, semplicemente disabilitiamola. Può trattarsi ad esempio dell'accesso remoto ad un router o ad una stampante di rete, oppure di un servizio di sistema attivato di default. Una volta terminata l'installazione di un sistema, il nostro

processo di hardening deve comprendere una valutazione dei servizi e dei demoni attivi, disabilitando ciò che è di troppo. Inoltre gli stessi servizi e demoni dovrebbero essere messi in bind esclusivamente sulle interfacce sulle quali effettivamente devono essere raggiunti.

Checklist di installazione

E' fondamentale avere ben chiara (e soprattutto documentata) una checklist di installazione delle workstation e dei server, in base alle diverse tipologie. Ad esempio, se installo un nuovo Linux, dovrò seguire una serie di step che contribuiscono a rendere il più sicuro possibile l'ambiente di lavoro. Questa attività inizia già in fase di installazione, impostando password sufficientemente complesse per l'accesso al bios della macchina, al boot loader e per i diversi utenti, partizionando correttamente i file system, installando solo i pacchetti necessari. Non dobbiamo inventare l'acqua calda ad ogni diversa installazione! Una volta definita la nostra checklist, per noi ed il nostro team l'installazione di una nuova macchina diventerà un'attività di routine che ci ruberà poco tempo e che ci permetterà di ottenere ottimi risultati.

Gestione device mobili

I devici mobili (smartphone, tablet, notebook) si perdono e vengono rubati. In ogni caso, è fondamentale avere una policy di gestione di questi dispositivi, applicando almeno delle politiche di sicurezza di base quali la possibilità di collegarsi remotamente al device (utilizzando un software di MDM) e poterne effettuare il wipe, la possibilità di localizzare il dispositivo, un pin di blocco di almeno 4 cifre, l'encryption del dispositivo. Se vogliamo spingerci più avanti possiamo avere anche il controllo delle applicazioni installate sui device e la distribuzioni di policy personalizzate utili ad esempo per il collegamento alla network wifi aziendale. È inoltre opportuno specificare una politica di gestione di questi device, sia essa la BYOD (Bring Your Own Device) o la COPE (Corporate Owned, Personal Enabled) e che documenti in modo puntuale l'eventuale trattamento di dati sensibili e/o riservati.

Two Factor Authentication

Da qualche anno a questa parte alcuni vendor (non tutti purtroppo) hanno capito che i prodotti devono essere rilasciati con alcune funzionalità di sicurezza facilmente configurabili oppure attive di default (security by desgn). La Two Factor Authentication (2FA) è una di queste. Abilitiamola, se possibile, oltre che sui vari account di servizi online (Gmail, Facebook, Amazon,…) anche sui dispositivi casalinghi, che sono sempre più spesso dotati di questa importante funzionalità.

Evitare il riuso delle password

Troy Hunt attraverso il suo sito HaveIBeenPwned ha reso pubblico anche alla massa il fenomeno del data breach. Ormai tutti (o quasi) stiamo iniziando capire che avere la stessa password per diversi servizi (o peggio, per tutti i servizi) è una cosa malvagia e assolutamente da evitare. Utilizziamo password diverse per servizi diversi o almeno suddividiamo i vari servizi ai quali accediamo secondo diversi livelli di riservatezza. Le credenziali di accesso al forum di giardinaggio probabilmente non hanno la stessa necessità di riservatezza delle credenziali di accesso ad Amazon...

Restringere lo user input

Quando abbiamo a che fare con la scrittura di web application è importante utilizzare una politica di controllo dell'input e di input sanitization al fine di evitare che la nostra applicazione possa essere utilizzata per accedere a dati che sono al di fuori dello scopo di quel determinato input.

Restringere lo user access

Il controllo di accesso deve essere applicato a tutti i livelli di entrata delle nostre reti, siano esse wired o wireless. Se non si riesce a fare di meglio il controllo può essere effettuato a livello di mac address (meglio che niente) o mantenendo disattivate a livello amministrativo le porte non utilizzante sugli switch (ed attivando ulteriori funzionalità di security quali il port security o il dhcp snooping), ma se si ha la possibilità di investire qualcosa, sia a livello economico che di tempo, è preferibile affidarsi ad una soluzione di Network Access Control (NAC).

In una medio/grande azienda, se la struttura fisica e l'ambiente lo permettono, è importante anche restringere l'accesso fisico alle varie aree aziendali, secondo profili personalizzati.

Applicare la need to known e la least privilege

All'interno di un'organizzazione, spesso per pigrizia o mancanza di sufficiente know how, si tende a lasciare che tutti i dipendenti/collaboratori abbiano accesso a tutte le risorse e le informazioni di proprietà dell'organizzazione stessa. Questo, se è accettabile in una piccola azienda, diventa particolarmente pericoloso nelle medie/grandi aziende. In questo tipo di organizzazioni più complesse è necessario configurare dei profili di accesso, a seconda dei diversi ruoli aziendali, che permettano alle persone di avere accesso esclusivamente alle informazioni ed alle risorse delle quali hanno bisogno per effettuare le proprie attività (need to know). Inoltre, sulle stesse risorse ed informazioni, devono essere applicati i minori permessi possibili (least privilege), garantendo ovviamente l'operatività ottimale.

Pianificare una risposta in caso di attacco

Se la nostra organizzazione ha iniziato la propria attività da almeno qualche mese non chiediamoci se prima o poi saremo vittima di un attacco informatico. Lo saremo certamente, probabilmente lo siamo già stati. Prima del successivo attacco è però necessario pianificare una risposta efficiente ed efficace. Dobbiamo pianificare e mettere nero su bianco una strategia di incident management, avendo lo scrupolo di censire tutti i vari scenari di incidente della quale la nostra organizzazione può essere oggetto (o almeno della quale pensiamo possa essere oggetto). Dobbiamo individuare chi all'interno dell'organizzazione sarà coinvolto nella gestione dell'incidente, chi sarà necessario informare, le modalità di documentazione dell'accaduto, le azioni da intraprendere in risposta all'incidente, la necessità o meno di rendere di dominio pubblico l'accaduto. La scrittura della strategia di gestione dell'incidente ci permetterà di gestire con meno stress una situazione che prima o poi ci vedrà sicuramente, nostro malgrado, protagonisti.

Monitorare nel continuo

Non importa quale software utilizzeremo per monitorare la nostra infrastruttura, l'importante è che il monitoraggio sia continuo ed in tempo reale. Per esperienza posso dirvi che sarà molto poco probabile che risolviate il discorso monitoraggio con un unico software, ma l'unione di più software potrà certamente soddisfare tutte le vostre esigenze. Personalmente mi sto trovando benissimo con una soluzione commerciale che integra diversi software open source quali Nagios/Icinga, lo stack ELK (Elasticsearch, Logstash, Kibana), Grafana, Influxdb. Un altro consiglio che posso darvi è quello di diffidare dei software proprietari che promettono di fare di tutto e di più. L'aspetto che trovo essenziale e fondamentale in un software di monitoraggio è la sua capacità di adattarsi totalmente all'infrastruttura da monitorare, oltre alla versatilità di configurazione. Per dirla in breve, devo essere in grado di plasmare il software secondo le mie esigenze, modificandone i check e scrivendone di nuovi se necessario. Inoltre devo avere la possibilità di creare delle dashboards facilmente leggibili ed interpretabili anche da chi non è il deux ex machina dell'infrastruttura. Non ultimo, uno degli aspetti fondamentali del sistema di monitoraggio è la capacità di allertare correttamente chi avrà poi il compito di sistemare le eventuali criticità rilevate. Non esageriamo con le notifiche, per esperienza se diventano troppe non vengono più prese in considerazione con la dovuta attenzione.

Effettuare verifiche periodiche

I VAPT (Vulnerability Assessment & Penetration Test) possono essere effettuati da personale interno o per conto di terzi. Non ha importanza chi li fa (a patto che siano soggetti con riconosciute capacità), l'importante è che queste verifiche si facciano! Personalmente prediligo che un'organizzazione, se opportunamente strutturata, abbia il proprio team di testing al proprio interno e che questo team effettui VAPT periodici (ogni 3

o 6 mesi), magari facendo effettuare VAPT, con periodicità più dilatate (1 o 2 anni), anche ad un team esterno all'azienda. I VAPT devono essere condotti seguendo una metodologia riconosciuta e facilmente replicabile (e che generi quindi risultati confrontabili) dai diversi soggetti che effettueranno l'attività. Due diverse metodologie che possono essere seguite e che sono fra loro complementari sono la OSSTMM (Open Source Security Testing Methodology Manual) e quanto contenuto nel documento NIST800-115 Technical Guide to Information Security Testing and Assessment, senza dimenticare, per la parte relativa alle web application, la metodologia OWASP (Open Web Application Security Project).

Avere un piano di formazione continuo

Non importa avere un'infrastruttura tecnologica e delle policy di sicurezza informatica di tutto rispetto, se poi lasciamo al proprio destino quello che rimane l'elemento più vulnerabile di ogni infrastruttura, vale a dire le persone. Tutto il personale (tutto!) deve essere formato adeguatamente e reso sensibile/consapevole dei vari aspetti di information security e delle minacce più diffuse in un determinato momento. Devono essere organizzati momenti di formazione periodici, anche più volte all'anno. Questi momenti alla lunga potranno sembrare ripetitivi, ma sono fondamentali proprio per trasmettere consapevolezza anche a quelle persone che non sono avvezze ai tecnicismi ma che comunque hanno a che fare con informazioni sensibili e/o riservate.

Cifrare il cifrabile

Tante, troppe volte vedo che nelle organizzazioni si tende ancora a fare largo uso di protocolli non cifrati, che permettono a potenziali attaccanti di recuperare facilmente, con un semplice sniffing di rete, preziose credenziali di accesso. È necessario rendere l'uso di protocolli cifrati parte di una policy aziendale. È inoltre un'ottima abitudine cifrare direttamente anche i dischi dei vari device che utilizziamo, siano essi pc o smartphone o quant'altro. Se proprio non possiamo abbandonare l'utilizzo di protocolli non cifrati per colpa di quella vecchia applicazione sviluppata da quella vecchia azienda chiusa da un pezzo, assicuriamoci almeno di restringere lo user access adeguatamente e di proteggere l'applicazione con delle acl ad hoc.

Backup, backup, backup (con segmentazione di rete)

Qualunque sia il problema catastrofico che colpirà la nostra azienda, nella maggior parte dei casi il backup sarà il nostro miglior amico. Sia essa una cancellazione avvenuta per errore oppure come conseguenza di un attacco o come conseguenza della diffusione di un cryptolocker, una politica di backup portata avanti correttamente può davvero salvare la nostra giornata (e non solo). Ricordiamo che la fase più importante di una politica di backup non è il backup stesso, ma il restore. Quindi testiamo frequentemente i nostri

backup effettuando dei restore di prova. Inoltre, per non appesantire l'infrastruttura di rete e se le nostre risorse ce lo permettono, è un'ottima scelta quella di riservare, per ogni hosts (o almeno per quelli più onerosi), un'interfaccia di rete per gestire i processi di backup. Ovviamente il traffico va poi segmentato anche sui diversi apparati di switching.

Documentiamo!

Non diamo per scontato che le altre persone capiscano quello che abbiamo implementato. Inoltre pensiamo sempre che l'organizzazione della quale facciamo parte deve poter sopravvivere in totale tranquillità anche senza di noi. È perciò importante documentare (con qualità) le varie implementazioni/configurazioni/policy che andremo ad effettuare. Così facendo risparmieremo del tempo prezioso in futuro (e scoccianti telefonate durante le nostre ferie!).

Applicare la defense in depth

Dobbiamo creare ridondanza attraverso diversi livelli di sicurezza, per far sì che la compromissione di un singolo livello non abbia un impatto catastrofico sulle informazioni presenti all'interno della nostra organizzazione. I vari punti esplicati in precedenza, se adottati correttamente e totalmente (o almeno in buona parte) ci consentono di creare diversi livelli che interagiscono tra loro e permettono di limitare notevolmente gli impatti in caso di attacco.

Impariamo dagli errori e non smettiamo di migliorare

Questo discorso vale un po' per tutti gli aspetti della vita lavorativa e non solo, ma vale certamente anche per ciò che riguarda la sicurezza informatica. Utilizziamo i nostri errori come base per la documentazione e appuntiamo di volta in volta come siamo riusciti a risolvere i problemi che abbiamo incontrato. Questo ci permetterà di costruire un database degli errori e delle relative soluzioni, che con il tempo diventerà preziosissimo. Seguiamo un ciclo di deming (PLAN – DO – CHECK – ACT) personalizzato per migliorare nel continuo le nostre policy.

Soddisfazione personale

Non sottovalutiamo l'aspetto psicologico positivo del creare (o almeno nel provare a creare) un'infrastruttura sicura. Per esperienza ci porterà ad avere quella piacevole sensazione di avere le cose sotto controllo e di conseguenza ci trasmetterà maggiore tranquillità nelle nostre attività quotidiane.

E infine confidiamo in un briciolo di buona sorte, che di certo non fa male!