Sicurezza IT: rimettere l'uomo al centro.

Fattori di Rischio

I rapporti sugli incidenti informatici ricordano che la Sicurezza di un ambiente IT è un discorso molto complesso e che abbraccia tutti gli aspetti della catena produttiva.

Innanzitutto c'è l'essere umano, che interviene in modo significativo in qualunque processo. Errore umano, perdita di conoscenze dovute alla perdita di personale chiave, e insufficiente preparazione o conoscenza delle criticità sono tutti fattori importanti di rischio, tali da poter addirittura vanificare i vari sistemi automatici di protezione messi in campo. Gli effetti sono di un danno colposo, non voluto, ma sempre di un danno.

Rilevante è anche la casistica di sabotaggi interni. Si va dalla negligenza colpevole al sabotaggio esplicito attraverso tutta una serie di gradazioni di interventi che hanno in comune la volontarietà di arrecare un danno. E anche in questo caso il fattore umano è rilevante.

Poi ci sono le rotture spontanee, ovvero i malfunzionamenti tecnici degli apparati, il cui fattore di rischio è inversamente correlato alla ridondanza degli stessi e all'adeguatezza dell'ambiente in cui operano, pesati per la criticità della parte di processo che vi si svolge.

Anche se sistematicamente sottovalutato, un grande fattore di rischio viene dai processi di cambiamento: dalla installazione di patch SW al cambiamento di HW, tutti questi interventi, se non pianificati con la dovuta cura e le dovute misure di protezione e regressione, sono una fetta consistente del rischio IT che si corre giornalmente. L'effetto è un danno colposo. Anche in questo caso il fattore predominante è quello umano.

Infine c'è quello che nell'immaginario collettivo è il solo e vero rischio sicurezza IT: l'intrusione esterna diretta o indiretta (quella per intendersi dovuta a cracking, virus, e tutti gli altri malware circolanti). I danni risultanti sono sempre di tipo volontario, anche se non necessariamente mirati contro un singolo individuo o azienda.

Metodi di riduzione del Rischio

Senza entrare nell'efficacia reale dei metodi che vedremo (perché ne discuteremo in seguito), è chiaro che dove il fattore umano è rilevante, si tende a minimizzare il rischio dovuto ad eventi non volontari con un miglioramento delle Procedure e una maggiore attenzione alla Formazione del personale.

Per quanto riguarda invece il rischio da eventi volontari, si tende ad introdurre sistemi più o meno automatici di Monitoraggio. Si tratta di sistemi di protezione passivi, ovvero di reazione, in quanto non fanno nulla per prevenire che il rischio si tramuti in danno, ma cercano semplicemente di minimizzarne gli effetti una volta che si sia presentato il problema.

Per ridurre la possibilità che il rischio di tramuti in danno, si introducono invece sistemi di Protezione. Si tratta di sistemi semiautomatici volti a prevenire (e per questo detti di protezione attiva) la possibilità che eventi considerati "non giustificati" possano verificarsi senza le opportune autorizzazioni, permettendo una riduzione del rischio.

Evoluzione del Rischio

Per comprendere quale sia la metodologia migliore per affrontare e ridurre i rischi di oggi e di domani, bisogna comprendere come questi si sono evoluti nel passato. Agli albori del personal computing (anni '80 e '90) lo scenario IT prevedeva fattori di rischio bilanciati tra le diverse concause che abbiamo visto in precedenza, eccetto per il fattore cambiamento e quello di intrusione esterna, che erano decisamente meno rilevanti degli altri. Questo per alcune ragioni importanti: l'interconnessione tra sistemi era molto inferiore rispetto ad oggi, i sistemi tendevano ad essere "congelati" per anni nelle loro configurazioni e la ragione per violare i sistemi era per lo più collegata alla volontà di singoli cracker di poter usare gratis risorse di calcolo o reti di navigazione più performanti, oltre che per dimostrare le loro capacità tecniche.

La situazione odierna è del tutto diversa, e i vari fattori di rischio sono tutti cresciuti e divenuti rilevanti. I sistemi vengono modificati su base mensile (con eccessi di aggiornamenti su base giornaliera), e questo di certo non permette la realizzazione di efficaci misure di fallback.

I vari malware e i tentativi di cracking sono finalizzati a scopi economici su larga scala, ovvero modi per accumulare ingenti ricchezze a scapito di altri (che si tratti del furto di identità o dell'accesso a informazioni riservate da rivendere a terzi). In più non si tratta più di attacchi generati da singoli, ma sempre più spesso da vere e proprie organizzazioni che si muovono con obiettivi precisi e strategie studiati a fondo, e che muovono ingenti risorse informatiche e finanziarie per raggiungere i loro fini. A conferma del cambiamento di scala vi è anche il fatto che molti paesi si sono dotati di unità di esperti informatici per la gestione di una guerra cibernetica. In questo scenario, il sabotaggio interno è diventato strumentale a fini dettati (e retribuiti) dall'esterno, e non più principalmente motivato dalla rivalsa per torti subiti sul luogo di lavoro o nella vita personale.

Anche i malfunzionamenti tecnologici hanno voluto il loro tributo di "notorietà" negativa: se infatti da un lato gli MTBF e l'affidabilità dei componenti sono aumentati in modo strutturale e significativo, dall'altro la mole di informazione, la complessità dei flussi e del processamento dei dati, insieme con la necessità di *uptime* sempre migliori ha ingigantito gli effetti di quelli che nel passato sarebbero stati considerati piccoli problemi.

Ad esempio: un tipico servizio utenti richiedeva negli anni '90 un uptime dell'85%. Oggi non è considerato accettabile un SLA sotto il 99.9%.

In tutto ciò, il fattore umano ha assunto una valenza ancora più importante: se infatti era frequente che un utilizzatore IT degli anni '80 e '90 avesse una comprensione informatica medio alta (ci ricordiamo cosa volesse dire usare il DOS?), oggi paradossalmente gli utilizzatori sono molti di più ma il livello di comprensione generale di come funziona un computer è diminuito significativamente. Ciò si traduce in una minore capacità di comprendere i rischi correlati con le proprie azioni. Siamo infatti tutti più bravi ad usare i programmi, ma comprendiamo molto meno cosa succede "sotto coperta". E questo è un grosso fattore di rischio.

Sistemi di protezione oggi

Il panorama della protezione IT odierna è molto ricco: offre tecnologie e strumenti neanche immaginabili solo 10 anni fa. Vediamone una breve carrellata.

A livello di prevenzione abbiamo:

- Firewall e screening routers: concetti noti anche all'utente domestico, sono modi per evitare intrusioni esterne al nostro sistema
- Antivirus, Ad-Aware, Anti-Spyware, Anti-Rootkit: tutti strumenti utili a prevenire l'istallazione o a rimuovere tempestivamente dal nostro sistema programmi o funzioni indesiderate;
- Anti-SPAM: sistemi per limitare l'impatto di messaggi di posta indesiderati;
- Sistemi di Crittografia o Steganografia dei dati, per prevenire che un eventuale accesso non autorizzato a informazioni importanti

Abbiamo poi sistemi IDS (Intrusion Detection Systems), che rappresentano un secondo livello di monitoraggio automatico, che cerca di rilevare le tracce di eventuali intrusioni che fossero riuscite ad eludere i sistemi di prevenzione.

Si tratta di tutti sistemi fortemente automatizzati (e che in alcuni ambienti IT non sono neanche disabilitabili dall'utente), che presentano spesso capacità euristiche notevoli.

Al livello di componentistica elettronica, i sistemi di ridondanza e affidabilità di base sono oramai una caratteristica stabile di tutti i sistemi ad uso non prettamente personale. Dalla presenza di alimentatori multipli ai vari sistemi RAID per i dischi, dal presenza di CPU multiple ai banchi di memoria con Correzione di errore, oramai l'affidabilità della parte "meccanica" ha fatto notevoli progressi, in modo anche economicamente competitivo.

Il proliferare di certificazioni di qualità (incluse quelle di sicurezza IT quali ISO27000) ha fatto aumentare anche la qualità dei sistemi di procedure, l'attenzione alla formazione e conseguentemente una maggior difficoltà per chi volesse espletare attività di sabotaggio interno.

Il Problema

Fin qui la teoria. Ma la realtà nasconde ben altre problematiche, che spesso vanificano gli sforzi profusi.

Procedure e Formazione. L'efficacia della protezione esercitata dipende in modo molto diretto dalla bontà e chiarezza dei processi produttivi, dei ruoli e relative responsabilità e dal budget che le aziende intendono impegnare. La realtà è che anche nelle aziende certificate, la presenza di procedure non ne garantisce affatto l'applicazione, e la formazione è più un optional o un dovere da espletare col minimo sforzo, anziché un progetto da seguire con attenzione. E allora tutte le problematiche di rischio si ingigantiscono. Infatti disattendere una procedura causa un rischio più alto che il non averla affatto, perché alcune cose sono date per scontate, senza verifica. Il caso di una realtà in cui nessuno faceva i backup, ma altri si comportavano come se ci fossero, poiché vi era una procedura per farli, è un tipico esempio dell'incremento di rischio.

Sistemi di Monitoraggio. La loro configurazione è tutt'altro che semplice, e il problema dei falsi positivi è reale, come altrettanto reale è la possibilità che questi facciano perdere credibilità al sistema, con tutte le implicazioni del caso. Nella maggior parte dei casi si tratta di grandi investimenti spesso lasciati funzionare senza che nessuno realmente curi agli allarmi che sono lanciati. E allora la falsa sensazione di essere protetti da un sistema automatico che però nessuno realmente ascolta, crea un rischio ancora maggiore che il non aver alcun sistema di monitoraggio. In tal caso infatti si nota una maggiore attenzione e consapevolezza del rischio.

Sistemi di Protezione. Tali sistemi sono tanto più efficaci quanto i processi di accesso, utilizzo e autorizzazione sono gerarchicamente organizzati in modo consolidato ed esclusivo, e, allo stesso tempo, la topologia e configurazione dei processi e dei flussi informativi è semplice e lineare. Purtroppo non è spesso così, tanto in azienda quanto in ambiente domestico. Nella prima, la presenza di sistemi eterogenei e di una crescita architetturale incrementale non ben programmata richiede la presenza di numerose eccezioni alle regole sicurezza e di sistemi legacy che divengono l'anello debole della catena. Nella seconda, il caso più tipico è proprio il PC di casa, in cui l'utente è anche amministratore, e spesso disabilita l'Antivirus quando non è in rete solo perché ritiene che rallenti il sistema, per poi dimenticarsi di riattivarlo quando si collega o inserisce un media esterno (CDROM, chiavetta USB, DVD…). E allora lui opera tranquillo e apre file senza pensare, tanto ha l'antivirus… Tutte cose che non farebbe se non lo avesse.

Ridondanza dei sistemi. Sebbene l' HW sia sempre più affidabile, ha bisogno di SW per funzionare. Dai microcontrollori programmati, al BIOS, fino alla ridondanza offerta a livello applicativo, la complicazione dei programmi ha introdotto un livello di rischio ulteriore che non viene spesso considerato.

Cambiamento. La complessità del SW e la sua diffusione a tutti i livelli dello stack produttivo ha introdotto una escalation del rateo di cambiamento. La necessità di applicare patch o aggiornamenti con sempre maggior frequenza e con minor tempo a disposizione ha causato una quasi totale eliminazione dei sistemi di verifica pre-rollout, nell'assunzione che i cambiamenti di SW ufficiali "funzionino sempre" e che il tempo dei test è sprecato. Una fiducia cieca molto rischiosa.

Una situazione simile si verifica anche nei progetti ad ampio respiro. Vi si sperimenta una sempre minore attenzione alla parte di test, a causa dei tempi limitati dettati da *time-to-market* sempre più ridotti e in cui spesso le fasi iniziali di design/sviluppo introducono ritardi che vanno proprio a scapito di quelle attività volte a garantire la minimizzazione dei rischi di cambiamento.

Nell'ambito delle intrusioni, si sperimenta una situazione di "back-firing", in cui chi produce sistemi di protezione "insegue" coloro che invece producono malware sempre più sofisticato. La presenza (ed il fiorente commercio) di un sempre maggior numero di attacchi "0-Day" è la comprova che in questo

processo, i sistemi IT sono sempre sconfitti, dal momento che ci sarà sempre un attacco che ancora non è noto a chi aggiorna i nostri sistemi, e che farà le sue vittime prima che si possa correre ai ripari.

Ma non basta: gli attacchi basati sul "Social Engineering" non sono in generale soggetti ad alcun tool automatico di protezione.

Cambiare strada

Negli ultimi 10 anni si è assistito ad un trend progressivo: l'esclusione dell'uomo dal controllo sulla sicurezza, assumendo che i programmi e le tecnologie fossero più affidabili e sicure.

L'evoluzione del rischio ha dimostrato che questa strada porta ad una battaglia persa in partenza, perché il fattore uomo è sempre più rilevante.

E allora bisogna cambiare rotta. Bisogna abbandonare l'approccio "reattivo" in cui l'obiettivo potenzialmente il pareggio, per un più strutturale sistema preventivo. Bisogna ricominciare a considerare che quel chilo e mezzo di materia grigia che è dotazione di ciascuno di noi è il computer più potente in assoluto, e che, se appropriatamente formato e supportato da tool, è in grado di prendere decisioni che nessun sistema informativo è capace di prendere.

Un esempio banale ma significativo lo troviamo nei sistemi di Anti-SPAM. Il nostro cervello impiega una frazione di secondo (e lo fa senza sforzo) per accorgersi che una mail con nel soggetto la frase "Via Ignora Questo Gra" è SPAM, mentre questo è un compito quasi impossibile per un programma antispam.

La stessa cosa si applica per tentativi di Phishing: una mail con il logo della nostra banca che mostra il testo di un link "Vai al tuo portale" e poi punta ad un sito qualunque invece che alla nostra banca è facile "preda" di un cervello preparato, mentre per un programma potrebbe essere un compito insormontabile.

E, ci sarebbero decine di altri esempi da fare, dall'amministrazione di sistema in reti aziendali fino al singolo PC di casa.

Chiaramente i sistemi informativi servono, ma devono essere trasformati in ausili all'uomo, ovvero sorgenti efficaci di informazioni e non elementi decisionali che ci propongono solo di confermare o rigettare azioni che loro hanno deciso. Ad esempio, un sistema di protezione delle mail ci dovrebbe segnalare che il 'From' mostrato è differente da quello reale dell'header di una mail (mostrandoli entrambi), per lasciar gestire a noi se quella è una mail falsificata o è corretto a causa di mail aliases o forwarding. Ad oggi, siamo noi a dover andare a guardare il lungo header per trovare questa informazione…

Si deve quindi puntare di più nel rendere l'uomo parte rilevante ("in control") del sistema IT, e non solo un suo utilizzatore. Facendo formazione mirata. Responsabilizzandolo. Ma soprattutto valorizzandolo.

Massimo Cardaci - info@edc-consulting.org