White paper

pronti a tutto

Business driven Security per l'era digitale

Creare fiducia e garantire conformità

La nuova alleanza tra obiettivi aziendali e necessità di sicurezza per la trasformazione digitale

Siete pronti a compiere con successo la trasformazione digitale? Ad accogliere in sicurezza e con affidabilità milioni di nuovi clienti? A promuovere apertamente lo sviluppo di nuovi ecosistemi affiliati? A finanziare con facilità modelli di business ancora inesplorati? In breve, siete pronti a trasformare fiducia e conformità in un nuovo pilastro del successo per la vostra strategia digitale? E siete pronti a far evolvere la sicurezza della vostra società da peso a generatore di profitti per l'era digitale?

Stiamo vivendo in un'epoca di paradossi. Sull'onda della trasformazione digitale, le opportunità di business non sono mai state tanto ricche. Tuttavia, queste opportunità comportano anche nuovi e quasi inimmaginabili rischi, e la grande maggioranza dei sistemi di sicurezza non è allineata. Uno sconcertante 90% delle aziende ammette di avere difese insufficienti. Recenti stime sui costi della criminalità informatica stanno già toccando quota 345 miliardi di USD all'anno, e i pericoli si aggravano giorno dopo giorno con l'avvento dell'Internet delle Cose, della stampa 3D e delle macchine intelligenti. Per certo, alcuni esperti sostengono che la stessa privacy diverrà un ricordo del passato.

Potrebbe sembrare che la sicurezza informatica nell'era digitale stia diventando una fatica di Sisifo. Potrebbe sembrare che le nostre società siano inevitabilmente nelle mani della Provvidenza, in un mondo che diventa ogni giorno più complesso, pericoloso e imprevedibile. Ma le aziende competitive riconosceranno questo momento come l'avvento di una nuova era che richiede un nuovo approccio alla sicurezza, nel quale questa non sia solo progettata per gestire tali elementi di incertezza, ma per essere il cuore pulsante della strategia di crescita digitale. Creare quindi una nuova alleanza tra sicurezza e business, di modo che le aziende siano pronte a cogliere le opportunità tanto quanto a difendesi dalle minacce.

Lo abbiamo sentito per anni: la digitalizzazione aumenta i rischi

Da Sony a Target, da JP Morgan alla Casa Bianca, le relazioni sugli attacchi illustrano quotidianamente i pericoli che le società di capitali e i governi devono parimenti affrontare. Senza dubbi, la sicurezza è diventata un problema spinoso con il convergere del mondo fisico con quello digitale. Non solo le minacce aumentano del 20% ogni anno, ma diventano sempre più grandi e incontrollabili. Gli hacker non sono più solamente quei pochi individui isolati con un hobby fastidioso; sono organizzazioni che lavorano ai livelli della mafia, dei gruppi terroristici e addirittura dello stato. E i rischi vanno ben oltre i 345 miliardi di dollari all'anno di danni a livello finanziario; essi mettono a repentaglio la vitalità di società di capitali e nazioni. Mentre il mondo diventa digitale, lo diventano anche i campi di battaglia economici e militari. Non c'è da stupirsi che gli analisti abbiano prospettato che, entro il 2020, il 25% delle aziende globali si avvarrà dei servizi di una organizzazione di "mercenari della guerra informatica".*

Tuttavia, mentre frodi, sabotaggi, estorsioni, spionaggio e rischi della guerra digitale non sono mai stati tanto elevati, in confronto la protezione non è mai stata tanto debole.

Il motivo? Se la digitalizzazione è determinante per il successo, la percezione generale è che i potenziali benefici siano più rilevanti dei rischi. Chiaramente, a molti può sembrare più importante creare immediati benefici con nuove applicazioni mobili o dispositivi connessi, con interconnessioni di nuovi ecosistemi o con l'ingresso nel cloud, piuttosto che attendere lo sviluppo dei necessari sistemi di sicurezza.

E di qui il grande divario: mentre i responsabili della sicurezza informatica (CISO) diligentemente consigliano maggior impegno nella sicurezza, la protezione semplicemente non sta crescendo di pari passo alla velocità e alle dimensioni dei rischi.

Ma tutto questo significa forse che dovremmo solamente attendere l'inevitabile, e riconoscere senza mezzi termini, come sostiene il Direttore dell'FBI James Comey, che

"ci sono due tipi di grandi aziende... quelle che hanno subìto un attacco informatico... e quelle che non sanno di averlo già subìto"?

Questo divario crescente tra rischi potenziali e misure concrete di sicurezza è la prova che ci serve per comprendere che, nell'infinita battaglia tra attacco e difesa, è arrivato il momento di un cambiamento di tendenza verso nuove strategie di sicurezza che possano abbracciare un mondo mutevole, aperto e imprevedibile.

*Fonte: Gartner

La fine della sicurezza come la conosciamo

Le nuove Golden Rules per la trasformazione digitale

Per anni, gli esperti di sicurezza hanno definito strategie, applicato tecnologie per la protezione e messo in opera processi di compliance. Le tecniche esistenti per la sicurezza restano fondamentali, tuttavia l'analisi delle migliori prassi dimostra sistematicamente che tre regole essenziali sono adesso di importanza vitale, tre norme molto semplici che sono il cuore della security nella nuova era digitale.

Regola 1: la sicurezza deve evolvere da orientata al rischio a orientata al business

Affrontiamo la verità: in un mondo digitale, l'utilizzo di una sicurezza a barriera è diventato un compito infinito. Come gestire ecosistemi composti da centinaia di partner, migliaia di impiegati, milioni di clienti e di cose, interconnessi e dispersi all'interno del cloud?

Naturalmente, protezione perimetrale multi-livello, Identity and Access Management federato, e sicurezza degli endpoint e delle applicazioni continueranno ad essere d'aiuto. Ma l'attenzione continua ad essere focalizzata su un enigma: quali saranno le risorse chiave da proteggere? Queste domande sono sempre state le preoccupazioni quotidiane dei responsabili della sicurezza informatica. Tuttavia, la sicurezza di domani richiederà un nuovo paradigma. Tutti i rischi possono essere valutati per deciderne la gestione: devono essere tollerati, trasferiti, trattati o terminati? Le società di capitali devono prendere seriamente in considerazione l'analisi dei loro rischi nella digitalizzazione:

- Uno scenario digitale accrescerà l'esperienza dei clienti o indebolirà la reputazione?
- Aumenterà l'eccellenza a livello operativo o creerà delle opportunità di dolo?
- Sosterrà il vantaggio commerciale o costituirà una minaccia alla proprietà intellettuale?
- Avrà un impatto sulla privacy e di conseguenza sulla fiducia dei consumatori, sulla compliance e sulle questioni legali?

Questi quesiti devono essere tuttavia costantemente fondati su una domanda centrale: qual'è il valore potenziale per l'azienda? In un mondo in cui la complessità aumenta, e la velocità digitale dello sviluppo rimane sempre un fattore essenziale, è vitale delineare delle politiche di sicurezza completamente orientate al business, utilizzando tabelle di valutazione, strumenti e stime altrettanto business-oriented e che coinvolgano tutti gli stakeholder.

L'opinione di Atos

di Alexis Caurette, Direttore della sezione Cyber Security Consulting & Integration, Big Data & Security di Atos

Noi di Atos crediamo che la mitigazione del rischio e la sicurezza siano una questione aziendale prima ancora che tecnica e di processo.
Per assicurare una sicurezza adeguata, è essenziale analizzare in profondità quali sono i rischi davvero critici dal punto di vista del business, e valutare le misure di protezione da tale punto di vista. Sebbene esistano da anni diversi metodi di bilanciamento del rischio, gli analisti stimano che solo il 20% delle aziende abbiano messo in opera un'efficace gestione del rischio. Per avere successo oggi sono indispensabili tre approcci:

1. Rendere la sicurezza un elemento chiave della strategia digitale, che metta costantemente in contatto sicurezza e business

L'obiettivo in questo caso è far sì che i Responsabili esecutivi prendano in considerazione la sicurezza nelle iniziative digitali, invece che considerarla un inibitore di business. Ad esempio, uno dei clienti di Atos, un'importante società elettrica, è stata in grado di accelerare la propria trasformazione digitale e soddisfare le esigenze di sicurezza e privacy dei clienti, integrando la sicurezza nella propria strategia di innovazione, e collegandola al valore aziendale. Il risultato? La crescita imprenditoriale è stata unita in modo completo alla fiducia dei clienti, quattro milioni di abitazioni sono state collegate in modo sicuro alla propria rete di contatori intelligenti ed è stata garantita la privacy dei dati personali di tutta la clientela.

2. Prendere in considerazione tutti gli ecosistemi e le catene di valore

Mentre i confini si confondono tra mondo digitale e fisico, tra società di capitali e partner, tra fornitori e clienti, le catene di valore della fiducia si stanno evolvendo rapidamente. Nel passato, le società di capitali sono spesso state accusate di lavorare con una cultura che distingueva tra "noi" e "loro". Queste frontiere si stanno dissolvendo. Di conseguenza, il pensiero olistico non è solamente utile, ma una necessità vitale. Per fare un ulteriore esempio, un altro cliente di Atos, un'azienda manifatturiera multinazionale, ha valutato i rischi della sicurezza all'interno del proprio intero ecosistema esteso, per semplificare la nuova generazione di identity and access management per milioni di clienti, fornitori, partner e dipendenti. Il risultato? L'incremento della sicurezza e della customer experience.

3. Mettere la fiducia e la privacy dei clienti al centro della vostra strategia

Con l'attuale rivoluzione digitale il cliente è posto nuovamente al centro. La sicurezza non deve fare eccezione, ma deve essere progettata per proteggere l'elemento più importante di una società di capitali: la propria clientela. Ad esempio, Atos ha supportato un Cloud pubblico indipendente europeo nel lancio di una offerta di cloud estremamente sicuro. L'impatto: non solo un elevato livello di protezione, ma una risorsa aziendale che sta aumentando le possibilità di business con imprese sensibili a livello di sicurezza ed enti pubblici.

Un trend innovativo

L'avvento delle cyber-assicurazioni, sia per l'IT che per le tecnologie operative (OT)

Deve essere tutto protetto? La risposta potrebbe non essere semplicemente sì o no. Esiste una terza soluzione, la cyber-assicurazione. Questo è un settore in crescita per i grandi gruppi assicurativi; in particolare si tratta di proteggere i clienti dai rischi dovuti alle normative, ed essere pronti per le imminenti leggi europee sulla privacy dei dati della clientela. Nessuno meglio delle società assicurative può comprendere quanto sia essenziale la quantificazione del rischio. Questo apre la porta a interessanti opportunità: una partnership tra assicurazioni e specialisti della sicurezza per verifica iniziale e potenziali indagini.

Questa è la scelta di assicuratori come Gras Savoye, che sta sviluppando con Atos una strategia di sicurezza end-to-end unica, un approccio con un forte valore aggiunto perché i cyber-attacchi non sono più limitati all'IT, ma prendono di mira anche l'OT, incluse le infrastrutture tecniche e gli oggetti smart connessi. Facendo forza sulla propria competenza industriale, Atos ha sviluppato una metodologia globale per aiutare le organizzazioni a identificare le proprie vulnerabilità, e a controllare e mitigare i rischi all'interno dell'IT e dell'OT. Sulla base dei propri standard di sicurezza per IT e OT, Atos è pertanto l'unico attore del mercato a mettere in totale sicurezza la catena di valore IT/OT. Tra gli esempi troviamo le auto connesse di Renault, i sistemi di pagamento con WorldLine, l'OT con Siemens, e l'elenco è ancora lungo.

Regola 2: dispiegare misure di protezione incentrate sui dati

Al momento attuale, i dati sono per certo la risorsa più critica del mondo digitale. Un tempo prodotto secondario delle applicazioni, i dati stanno rapidamente diventando il capitale primario delle aziende. Con l'emergere dell'Internet delle Cose, stiamo entrando in un mondo nel quale l'intelligenza universale integrata trasformerà qualsiasi oggetto in un dispositivo smart. E il fattore che unirà tra loro persone, processi e cose, sono i dati.

Log, conversazioni, transazioni... i dati stanno diventando la nuova risorsa che alimenterà l'economia di domani, come la finanza fece nel secolo scorso. La posta in gioco è una migliore comprensione del comportamento dei clienti, una migliore capacità di ottimizzare i processi aziendali in tempo reale, e nuove percezioni che possono essere scambiate, barattate o addirittura vendute per creare nuovi modelli di business. Le società di capitali basate sulle informazioni sono già il 20% più redditizie e ottengono il doppio del valore di mercato di società simili.

Nessuna sorpresa se i dati sono adesso l'obiettivo degli attacchi informatici. Come dimostrano i casi di Sony e WikiLeaks, la perdita di dati è una delle questioni più pressanti del momento.

Le conseguenze sono chiare: in un mondo digitale in cui i dati costituiscono il valore aziendale primario, questi devono essere anche al centro della sicurezza dell'impresa.

Un trend innovativo

La Data Loss Prevention (DLP) basata sul Cloud come servizio

Cosa dovrebbe preoccupare di più le aziende, proteggere dati critici da minacce interne, o proteggere il business da cyber-criminali organizzati che cercano di vendere i loro IP al maggiore offerente? Per rendere facilmente disponibili i servizi avanzati di Data Loss Prevention, Atos ha lanciato un innovativo servizio DLP basato sul cloud, utilizzabile da qualsiasi parte del mondo e che permette rapida fruibilità e scalabilità su tempi di ammortizzazione brevi. Questo servizio cloud completamente gestito comprende il Security Operation Center di Atos e la nostra esperienza in DLP, per offrire un'efficace gestione del rischio e una robusta prevenzione ai furti di dati, sia da attività interne non autorizzate che da minacce esterne.

L'opinione di Atos

di Gerrit Pot, Global Offering Manager, Cyber Security di Atos

Noi di Atos crediamo che le politiche di sicurezza dei dati richiedano un'estensione delle attuali strategie di security. Ovvero, non è necessario solo revisionare le politiche, ma anche l'architettura e gli strumenti, dagli end point alle infrastrutture. Per riuscirci con successo, sono indispensabili tre approcci:

1. Rompere i silos per assicurare un approccio alla sicurezza olistico e incentrato sui dati

Una massima che circola negli ambienti della sicurezza dice: perché usare un portone blindato se poi lasci la finestra aperta? Troppo spesso i dati sono sparpagliati all'interno di molteplici database con diversi processi. Una stima di Gartner sostiene che "nel 2016, oltre l'80% delle organizzazioni non riuscirà a sviluppare una politica di security dei dati consolidata nei silos, con potenziali rischi di non-compliance, brecce nella sicurezza e responsabilità a livello finanziario". Atos ha sviluppato delle metodologie specifiche per gestire questa sfida. Ad esempio, abbiamo aiutato un'importante azienda multinazionale a proteggere i dati strategici all'interno dei silos progettando una avanzata Application Resource Island. Il risultato? Informazioni preziosissime disponibili per il business che hanno apportato svariati miliardi di Euro in ricavi, ma tenuti sotto stretto controllo e monitorati in modo sicuro.

2. Dispiegare tecnologie data-centric

Al di là della crittografia, del data masking, delle tecnologie di DCAP (Data-Centric Audit and Protection, protezione e verifica centrate sui dati) e così via, sono necessari nuovi livelli di identity and access management contestuale. L'utilizzatore è la persona giusta con il ruolo legittimo che gli permette di accedere ai dati esatti per eseguire le azioni appropriate? Devono essere esaminati sia il contesto che il comportamento, in modo che gli appositi motori di correlazione siano in grado di prendere le decisioni più adatte.
Atos è stato di supporto a diverse tra le più grandi banche europee nel mettere in opera sistemi di sicurezza di alto livello per i trading desk, permettendo il risparmio di miliardi di dollari.

3.Prendere in considerazione l'evoluzione del ciclo vitale dei dati

I dati aziendali non sono materia inerte, bensì un organismo vivente. Ad esempio, dati non sensibili possono essere messi in correlazione per diventare sensibili, e dati archiviati possono essere richiedere una declassificazione dopo qualche tempo.
La sicurezza dei dati deve prendere in considerazione questa evoluzione, e passare da una valutazione statica a una dinamica. Ad esempio, Atos ha consegnato una soluzione di sicurezza data-centric a una società farmaceutica leader mondiale, per far sì che i dati di ricerca & sviluppo siano monitorati in sicurezza, evitando perdite di IP che potrebbero comportare costi per miliardi.

Regola 3: evolvere ad una gestione proattiva e in real time delle indagini di sicurezza

Il crescente mondo digitale non è solo più complesso, è anche più veloce. Negli anni settanta e ottanta, ci sono voluti 18 anni per mettere insieme i primi 50 milioni di utilizzatori di telefoni cellulari, ma all'inizio di questo decennio a Google+ sono bastati 3 mesi. E il ritmo è ancora in accelerazione.

Di conseguenza, è ancora più difficile prevedere futuri problemi e opportunità. La sicurezza può essere stata ben pianificata in passato, ma non può essere immune a nuove tipologie di attacchi sconosciuti. Pertanto, in un mondo sempre più complesso che si evolve in tempo reale, è essenziale ri-indirizzare i budget per la security da una protezione generica a risposte rapide di rilevamento e reazione. Le nuove strategie di sicurezza devono adattarsi a un mondo sempre più insitamente imprevedibile e in real-time, un mondo nel quale essere in grado di reagire all'ignoto, o addirittura cercare di prevederlo, sarà una questione di vita o di morte.

I meccanismi di security in tempo reale saranno necessari per monitorare costantemente e identificare attività sospette, contrattaccare senza ritardi e attivare immediate azioni di risanamento. Sarà un nuovo approccio alla security di tipo "defcon" (condizione di sicurezza) e preventivo, la cui importanza primaria per la gestione operativa è sottolineata dall'avvento della prossima generazione di Security Operation Centers e strategie di indagine.

L'opinione di Atos

di Zeina Zakhour, Direttore Tecnico per la Cyber Security, Big Data & Security di Atos

Noi di Atos crediamo che la sicurezza stia diventando sempre più una sfida per i Big Data: non solo come percepire e rispondere alle minacce in tempo reale, ma ancor di più, come evolvere da security reattiva a proattiva, e addirittura a preventiva? Per riuscirci con successo, sono indispensabili tre approcci:

1. Creare un processo di governance della sicurezza in tempo reale

Gli Advanced Security Operations Centers (SOC) e il Security Information & Event Management (SIEM) devono essere integrati alle nuove strategie di sicurezza. In particolare, Atos ha creato l'Atos High Performance Security, una rete avanzata di SOCs/CSIRTs (Computer Security Incident Response Teams) per rispondere a questa esigenza "come servizio", basandosi sulle ultime percezioni in merito a minacce e ambienti di protezione. Serviamo molte delle più grandi e maggiormente sensibili società di capitali di tutto il mondo, e offriamo protezione 24/7 e reazioni immediate, come dimostrato durante gli ultimi Giochi olimpici, durante i quali centinaia di milioni di minacce hanno portato a zero violazioni. Atos supporta inoltre le aziende che desiderano utilizzare i propri SOC privati per schierare avanzati centri operativi di sicurezza indipendenti.

2. Utilizzare team investigativi

I team investigativi endpoint saranno sempre più necessari per analizzare e classificare grandi quantità di informazioni informatiche digitali, e per trovare catene di indizi che possano essere usate nei tribunali. Insieme ai SOC, devono unire competenze internazionali e locali, per gestire contesti e regolamenti regionali. Ad esempio, Atos sta aiutando i propri clienti a contenere rapidamente e in modo efficace attacchi mirati per limitare l'impatto sul business. I team investigativi CSIRT di Atos eseguono inoltre procedure di reverse engineering sui tentativi di intrusione per tracciarne gli esecutori, raccogliere prove e assicurarli alla giustizia

3. Passare da sicurezza reattiva a preventiva

Mentre oggi la maggior parte del lavoro investigativo deve rispondere ai crimini dopo che sono stati compiuti, nei prossimi anni sarà sempre più vitale predisporre controlli in tempo reale per prevenire cyber-attacchi (sicurezza proattiva) e anticipare le minacce (sicurezza preventiva). Ad esempio, Atos ha implementato per un cliente internazionale una soluzione avanzata e costante di rilevamento e rimozione delle minacce, in grado di rilevare attacchi mirati sin dal Giorno Zero. Non solo il SOC di Atos rileva in tempo reale attacchi sconosciuti e diffusi, ma fornisce i meccanismi automatici per bloccare e neutralizzare tali attacchi, in pratica azzerando l'impatto sull'azienda.

Un trend innovativo

L'avvento delle cyber-assicurazioni, sia per l'IT Le statistiche dei Big Data al cuore della prossima generazione di Security Operation Centers (SOC)

Miliardi di log, milioni di utenti: con i SOC e i SIEM la sicurezza ha fatto il proprio ingresso nell'era dei Big Data. Poiché le minacce salgono sempre di livello e gli attacchi sono sempre più complessi, per individuarli è necessario un nuovo approccio. Le società avranno bisogno di un sistema avanzato di sicurezza predittiva e security intelligence sensibile al contesto e operativa, che utilizzi il potere dei dati analitici di terza generazione per rilevare schemi sospetti.

Utilizzando gli event log feed usati dai SIEM tradizionali e unendoli con numerosi nuovi data feed, Atos sta sviluppando un apprendimento automatico di ultima generazione e delle analisi di tipo bayesiano che permettano un'analisi profonda e portino a scoprire delle minacce costanti evolute (Advanced Persistent Threats, APT). Inoltre, Atos ha sviluppato dei servizi di threat intelligence che navigano nelle profondità del web e in altri forum underground per cercare allerte precoci e schemi di minaccia sconosciuti. Mettendo in correlazione servizi di monitoraggio e threat intelligence, possiamo fornire analisti e soluzioni di sicurezza con una visione predittiva sull'evoluzione delle minacce e sul potenziale impatto sul business, che permetta una protezione preventiva per la maggior parte delle categorie, dalla sicurezza nazionale alla gestione delle frodi finanziarie e dei furti nelle aziende di servizi pubblici.

Costruire la fiducia, fare leva sulle opportunità

Nella vita di tutti i giorni, la prima leva del business è sempre stata la fiducia. Puoi fidarti del venditore con il quale stai trattando? Nel mondo digitale, questo è sempre stato un importante elemento di preoccupazione, ma l'avvento dell'Internet delle Cose lo ha rivestito di una nuova dimensione.

Quando comunicate i vostri dati personali a una società di telecomunicazioni che quindi conoscerà tutto di voi e della vostra vita; quando affidate le vostre risorse finanziarie a una banca che potrebbe cancellarle in pochi millisecondi nelle proprie reti di trading ad alta velocità; quando governate la vostra casa con dispositivi intelligenti i cui sensori potrebbero essere hackerati; quando mettete la vostra vita nelle mani di un'automobile che si guida da sola il cui software potrebbe essere sopraffatto da un malware; quando la vostra stessa vita potrebbe dipendere un domani da dispositivi medici connessi quali sistemi di cuore artificiale; allora vi serve una fiducia assoluta.

La sicurezza è, in questo senso, a un punto di svolta.

Non solo è necessaria per ridurre i rischi e assicurare la conformità alle normative. Diminuendo i rischi, le società di capitali possono assumere potere: sono più affidabili, più agili e portano il business a nuove altezze. La sicurezza diventa una risorsa primaria per l'azienda, poiché offre un valore tangibile alle società di capitali che cercano di conquistare i territori inesplorati del mondo iper-connesso.

In questo modo, la cyber-sicurezza **non è solo la chiave per affrontare pericoli imprevisti, ma anche per fare leva su opportunità di business altrettanto inattese**.

- Essere in grado di accettare milioni di nuovi clienti
- Essere sufficientemente agili da finanziare lo sviluppo di inaspettati ecosistemi consociati su piattaforme API sicure.
- Essere abbastanza perspicaci da fare leva sulle necessità di nuovi modelli di business nell'emergente economia dei dati

Di certo, nell'imminente età digitale, così come i dati stanno diventando la nuova valuta, la fiducia può essere considerata la risorsa aziendale più intangibile. Per anni, i sistemi di valutazione hanno mostrato come le aziende nei settori della vendita al dettaglio e del turismo possono dipendere dalla reputazione. Nel mondo iper-connesso di domani questo concetto sarà portato a un nuovo livello.

In poche parole, al di là della protezione, la sicurezza sta diventano una nuova risorsa aziendale all'interno del viaggio digitale. Una risorsa che:

- Accrescerà **la customer experience** - facilitando un accesso sicuro e senza problemi alle informazioni, e assicurando la fiducia dei clienti in merito alla privacy dei dati
- Aumenterà **l'eccellenza operativa** - facendo sì che le catene di valore aziendali non siano a rischio (dalla produzione alla distribuzione al servizio clienti)
- Supporterà **il rinnovamento del business** – garantendo innovazione e proteggendo la risorsa più preziosa: i dati

Si tratta di una mossa strategica per la cyber sicurezza e una rivoluzione copernicana che trasformerà la security da peso e centro di costo per le aziende, a generatore di ricavi.

Sicurezza: pensare globale, agire in verticale

Dispositivi e piattaforme digitali hanno creato molteplici opportunità per permettere a organizzazioni di tutte le dimensioni, e di tutti i settori industriali, di guadagnare un margine competitivo. Il digitale sta ora svolgendo un ruolo fondamentale nel business aiutandoci a lavorare, a distinguerci e a comunicare in nuovi modi.

Tuttavia, per qualsiasi potenziale ricompensa, esiste una potenziale minaccia. Bilanciare l'accesso a sistemi, reti e dati critici con sicurezza, controllo e gestione, costituisce una sfida costante. E poiché le minacce alla sicurezza evolvono e mutano costantemente, questo bilanciamento non è mai definitivo. La sicurezza digitale è una questione globale.

Tuttavia, quali sono le caratteristiche specifiche per ciascuna categoria? Sebbene le soluzioni che molte società adottano siano universali (gestione dei criteri di protezione, identity and access management, sicurezza delle comunicazioni, SOC...), il livello di protezione e i rischi aziendali specifici variano enormemente all'interno dei settori e delle organizzazioni industriali.

Il settore finanziario è particolarmente esposto alle minacce.
Oggi è riconosciuto quale obiettivo principale del cyber-crimine. Operatori insoddisfatti hanno inoltre recentemente dimostrato come si possano usare gli accessi digitali per manipolare i centri finanziari. Gli impatti devastanti che ne sono derivati hanno avuto come conseguenza l'imposizione di elevatissime misure di sicurezza per i trading desk.

L'influenza delle loro azioni va ben al là del dipartimento IT: hanno infatti generato importanti sfide per le aziende, e innescato profonde revisioni della compliance e dei regolamenti, sia a livello locale che globale. Gli analisti dell'industria stimano che il 50% del budget delle banche per l'IT potrebbe subire conseguenze da regolamenti quali le norme antiriciclaggio (Anti-Money Laundering Act), la normativa FATCA (Foreign Account Tax Compliance Act), la legge Dodd-Frank, gli stress test e la Basilea II. L'avvento delle nuove tecnologie di criptovaluta potrebbe comportare enormi e dirompenti sfide nell'immediato futuro.

Quello dei media e delle telecomunicazioni è un altro settore in prima linea nel problema della sicurezza. La loro pubblica visibilità li rende un obiettivo evidente, con minacce sia all'integrità dei dati (deturpazione per propaganda), alla disponibilità (attacchi mirati all'interruzione del servizio) o alla confidenzialità (inclusi dati della clientela). Non mancano le sfide specifiche, come la gestione dei diritti digitali (DRM).

Energia e servizi di pubblica utilità potrebbero vedere un incremento delle minacce nei prossimi anni. Per quanto riguarda i servizi di pubblica utilità, l'aumento delle smart grid, dei contatori intelligenti e delle case domotiche stanno creando immense opportunità per aziende e consumatori, ma anche occasioni per cybercrimini e abusi. Le tecnologie operative sono degli obiettivi particolarmente ricercati. Quando si parla di guerra informatica, non sorprende che i servizi di pubblica utilità siano riconosciuti come uno degli obiettivi potenziali più strategici, e pertanto necessitino delle strategie di protezione più rigorose.

Le società produttrici di petrolio e gas devono proteggere i dati della clientela e schermare risorse vitali dalle minacce del cyber-terrorismo, allo stesso tempo rispondendo in modo puntuale e trasparente a obblighi normativi di informativa sempre maggiori, come ad esempio la compliance a livello sociale e ambientale.

La vendita al dettaglio ha subito frequenti attacchi a livello di front office, con minacce in forma di truffe o ricatti. Sfortunatamente queste minacce non svaniranno mai. Inoltre, l'ascesa delle catene di valore integrate delle 3 D (orientate alla Domanda, basate sui Dati ed eseguite in modo Digitale) e la connettività degli oggetti faranno diventare il settore **manifatturiero** e quello dei **trasporti** i prossimi obiettivi strategici del cyber crimine. Saranno quindi necessarie misure di protezione altamente specializzate, in particolare per l'Internet delle Cose, l'apprendimento automatizzato, l'intelligenza artificiale e la sicurezza robotica.

Anche la sanità è a rischio. L'aumento dei progetti di "salute connessa" offre opportunità agli attacchi digitali. Compromettere i dati riguardanti la sanità potrebbe minacciare direttamente la vita stessa. Questo potenziale lo rende uno dei settori più critici per il futuro della sicurezza.

Il settore pubblico non è immune dal cambiamento epocale portato dal digitale, sia a un livello proprio (con i processi di digitalizzazione e gli open data) che come elemento critico fondamentale per tutti gli altri settori, come la difesa e la sicurezza nazionale, le normative, la giustizia e i servizi di pubblica utilità. In complesso, rappresenta un terreno molto fertile per il cyber-terrorismo, e le questioni di sicurezza non devono solo essere trattate individualmente, ma anche all'interno di un contesto di fiducia e compliance più globale, che vada al là di settori quali la gestione del rischio, la sicurezza delle transazioni, la prevenzione delle frodi, la progettazione di sistemi critici, la governance della conformità e i requisiti normativi.

Grazie all'unione ininterrotta tra business e pensiero tecnologico, Atos ha posto questo approccio al cuore della propria offerta per la trasformazione digitale di tutti i settori.

Conclusione

In questo nuovo mondo, la sicurezza non sarà più la stessa. Per avere successo, le aziende devono cambiare la loro attitudine mentale verso la security, adottare nuove "regole" di sicurezza e abbracciare un nuovo approccio olistico con:

- Gestione del rischio selettiva incentrata sul business
- Strategia di protezione data-centric
- Maggiori investimenti in sicurezza e indagini preventive
- Sicurezza orientata al business per prepararsi all'imprevedibile

La cyber-security di Atos: una nuova tipologia di partner

Per avere successo, le aziende avranno bisogno di un nuovo tipo di partner. Un partner che unisca sicurezza e business all'interno di un approccio coerente di trasformazione digitale. Un partner che valuti e gestisca i rischi insieme all'intera catena del valore, dai dispositivi connessi alle infrastrutture. Un partner che crei strategie incentrate sui dati. Un partner che le cui strategie di sicurezza siano evolute da reattive a preventive, con servizi di indagine e SOC in tutto il mondo. In poche parole, avranno bisogno di società che uniscono intrinsecamente sicurezza e business, attività di consulenza e operatività, servizi e tecnologia. Per far si che la fiducia non sia solo una risorsa difensiva, ma una vera e propria leva per il valore aziendale.

Atos è una società leader in servizi digitali, con 93.000 dipendenti che operano in 72 paesi. Quale partner fidato per la trasformazione digitale, Atos supporta grandi società di capitali e governi ad assicurare fiducia e compliance orientati al business e senza compromessi.

Quale leader mondale nella cyber sicurezza integrata, Atos fornisce una protezione end-to-end senza eguali, che comprende:

- Gestione della sicurezza globale del ciclo vitale aziendale, da attività di consulenza a servizi gestiti di cyber sicurezza, con oltre 4.500 specialisti e otto Security Operations Centers in tutto il mondo, operativi 24 ore su 24, 7 giorni su 7
- Competenza nella sicurezza IT/OT globale all'interno delle catene di valore digitali, da oggetti connessi e applicazioni in cloud, a piattaforme di back-office e infrastrutture IT vitali
- Competenza nella sicurezza aziendale globale all'interno di mercati specifici, dal manifatturiero, retail e trasporti, al finanziario, telecomunicazioni, media, servizi di pubblica utilità, pubblica amministrazione e sanità.

L'expertise di Atos si fonda su oltre 25 anni di esperienza nell'offrire alle organizzazioni più esigenti soluzioni e servizi per la sicurezza efficaci, completi e adatti allo scopo. Si basa anche sull'acquisizione nel 2014 di Bull, una rinomata società nel campo della difesa e dei Bid Data, con soluzioni avanzate per l'identity and access management, la sicurezza di dati analitici, la crittografia e i sistemi critici per la difesa e il settore aerospaziale. Di conseguenza, grazie al proprio vasto ecosistema di partner, Atos non offre solo la più ampia gamma di tecnologie di security per creare e gestire soluzioni di sicurezza idonee, su misura e orientate al business, ma propone anche tecnologie rivoluzionarie nel momento in cui sono necessarie soluzioni di sicurezza di alto livello e indipendenti.

Il fiore all'occhiello delle innovazioni di Atos include Worldline, la principale piattaforma europea di pagamento e transazioni sicure; Hoox, il primo smartphone a sicurezza integrata del mondo; sistemi di sicurezza avanzati per oggetti smart connessi alle auto o alle Smart Grid; sistemi di sicurezza avanzati per i trading floor; e infine sistemi di security estrema per i settori più critici quali la difesa, il nucleare e l'aeronautica. Ogni giorno milioni di vite sono protette dai sistemi di difesa critica di Atos, 13 milioni di transazioni sono gestite da Worldline, 100 milioni di identità sono amministrate in modo sicuro dalle tecnologie IAM di Atos, e due miliardi di eventi di security sono analizzati dai SOC di Atos. Il risultato? Centinaia di miliardi di euro in business digitale protetti ogni giorno.

Agite subito

Scoprite in quale modo Atos potrebbe essere il partner che vi serve, partecipando a uno dei workshop sulla valutazione o sull'innovazione. Potrete imparare come abbiamo aiutato altre organizzazioni a misurarsi con nuovi tipi di esposizioni, e ricevere qualche informazione aggiuntiva in merito alle più recenti migliori prassi in materia di cyber security.

Potete anche richiedere una consulenza gratuita, come l'Atos Security Scan. Durante queste sessioni possiamo valutare lo stato attuale della vostra posizione in merito alla sicurezza, e determinare se sia adatta allo scopo sulla base delle recenti ed emergenti minacce.

Per saperne di più:
www.atos.net/security

Chi siamo

Atos SE (Societas Europaea) è leader nei servizi digitali con un fatturato annuo pro forma 2014 di circa 12 miliardi di EUR e 100.000 dipendenti che operano in 72 paesi. Con clienti a livello globale, il Gruppo fornisce servizi di Consulting & System Integration, Managed Services & BPO, Cloud Operations, Big Data & Cybersecurity solutions e Transactional Services attraverso Worldline, leader europeo nel settore dei pagamenti e servizi transazionali. Grazie alla sua comprovata esperienza tecnologica e a una profonda conoscenza industriale, il Gruppo vanta clienti in molteplici settori industriali: Difesa, Servizi Finanziari, Salute, Industria Manifatturiera, Media, Servizi di pubblica utilità, Pubblica Amministrazione, Retail, Telecomunicazioni e Trasporti.

Atos è focalizzata sulla tecnologia di business che alimenta il progresso e aiuta le organizzazioni a creare la loro impresa del futuro. Il Gruppo è il Worldwide Information Technology Partner dei Giochi Olimpici e Paralimpici ed è quotato al Mercato Euronext di Parigi. Atos opera con i brand Atos, Atos Consulting, Atos Healthcare, Atos Worldgrid, Bull, Canopy, Unify e Worldline.