ADVNET | ADVANCED THINKING

Vincere la guerra ai Ransomware e proteggere i propri dati.

L'approccio Advnet

IMMUTABILITA'

Best Practices per un'azienda resiliente

"Advnet è consapevole che non basta un buon firewall o un buon antivirus per contrastare efficacemente le cyber-minacce moderne."

La protezione dei dati dei clienti è una delle nostre mission principali. Per raggiungere lo scopo sappiamo che bisogna adottare una serie di contro-misure adeguate.

Seguire queste 6 best practices certamente mitiga il rischio elevando la sicurezza ad un livello impensabile fino ad oggi.

01 ANALISI DELL'ARCHITETTURA IT E DATA GOVERNANCE

Il primo step è capire quali sono le possibili vulnerabilità della nostra infrastruttura IT, quali sistemi erogano i servizi acceduti dagli utenti e con quali privilegi gli utenti e gli amministratori interagiscono con essi.

Capire per tempo i propri punti deboli è il primo passo per porre in atto dei tasks di remediation. Mettere in campo una soluzione di Data Governance significa, oltre ad essere compliance con la normativa GDPR, capire dove i dati di valore della nostra azienda risiedono, chi vi può accedere, con quale livello di privilegi, come questi dati si muovono dentro e fuori l'azienda e, soprattutto, come meglio proteggerli.
Auditor - GDPR

02 "ZERO" TRUST e PRIVILEGI MINIMI

Gli attaccanti che riescono a sfruttare le vulnerabilità per accedere ai sistemi aziendali devono comunque trovare il modo per entrare in possesso di credenziali privilegiate per poter creare un danno permanente al sistema.

"ZERO" TRUST vuol dire, in parole semplici, verificare SEMPRE l'identità di chi accede ai servizi IT della nostra azienda.

A maggior ragione la verifica dell'identità e le regole di accesso devono essere più stringenti per chi ha responsabilità amministrative nella gestione del sistema informativo aziendale. Il nuovo modello di riferimento deve divenire quello dei MINIMI privilegi (LEAST), ov-

vero assegnare a ciascun utente soltanto il set minimo di diritti necessari per svolgere il proprio lavoro, soltanto per il tempo necessario per farlo e soltanto verso i sistemi con cui deve interagire. Il vecchio modello per cui il Domain Admin poteva essere utilizzato in ogni occasione deve scomparire.

03 STRONG AUTHENTICATION

L'accesso ai sistemi aziendali, soprattutto quelli più critici, dovrebbe avvenire attraverso l'introduzione di sistemi di strong authentication personali a più fattori, anche biometrici, così da mitigare il rischio legato alla sottrazione fraudolenta delle credenziali utente, in particolare il phishing. Un sistema di autenticazione a più fattori deve poter quindi integrare efficacemente informazioni che conosciamo soltanto noi a qualcosa che possediamo in via esclusiva (token, smartphone, impronte digitali, etc.) così da rendere l'accesso ai sistemi aziendali estremamente più sicuro. **Strong Authentification**

04 WINDOWS LIFECYCLE

Gennaio 2020 è il mese della fine del supporto per i vecchi sistemi legacy Windows 7 e Windows Server 2008. Il nuovo modello Microsoft è legato al sistema Windows 10 che non può più essere definito semplicemente un Sistema Operativo, bensì come una soluzione SaaS (Software as a Service).

Come tale, le builds di Windows 10 vengono rilasciate semestralmente e non tutti gli amministratori IT sanno che hanno una scadenza del supporto differente, 18 o 30 mesi.

Questo significa che, sebbene tutti i PC siano stati migrati a Windows 10, col passare dei mesi e degli anni, se non si è intrapresa una politica corretta di mantenimento del ciclo di vita di Windows 10, è molto probabile che buona parte dei PC siano già fuori supporto Microsoft, lasciando aperti gli accessi ad eventuali vulnerabilità che possono essere sfruttate dai cyber-criminali. Gestire il ciclo di vita dei sistemi operativi diventa quindi una operazione fondamentale.

ADVANCED THINKING

Advnet esiste per permettere alle aziende di essere competitive ed innovative grazie al miglior utilizzo possibile della tecnologia IT.

Seguiamo l'azienda in tutte le fasi attraverso un team di professionisti dalle elevate skill e servizi di assistenza personalizzata, frutto di anni di esperienza e riconoscimenti.

05 FORMARE I DIPENDENTI

La formazione dei dipendenti è una strategia fondamentale per ridurre la capacità di attacco dei cyber criminali. Molto spesso il ransomware è introdotto in azienda proprio da un semplice click su un link creato ad hoc in una mail di phishing o tramite un pezzettino di software scaricato da qualche sito precedentemente compromesso. I dipendenti devono comprendere quindi di essere il target privilegiato di questi attacchi e di conseguenza essere aiutati a riconoscere il pericolo che potrebbe derivare dalle proprie azioni lavorative quotidiane. **Vulnerability Assessment**

06 POSSEDERE UNA COPIA SICURA, RECENTE E NON COMPROMESSA DEI PROPRI DATI

L'importanza di possedere un sistema di backup integro e funzionante, che permetta di recuperare tutti i dati oltre che l'operatività aziendale, a fronte di attacchi di tipo Ransomware, è quasi superfluo sottolinearlo.
Questo vuol dire avere una copia dei dati offline, non raggiungibili dalla rete, su un supporto sicuro e possibilmente WORM.
Non solo, la copia dei dati su questi dispositivi dovrebbe essere anche la più recente possibile. Recuperare da un attacco Ransomware dati vecchi di mesi da un supporto offline dimenticato in qualche cassetta di sicurezza per lungo tempo potrebbe non essere comunque una soluzione. Se i cyber-criminali sviluppano nuovi ransomware, alzando sempre di più l'asticella della protezione e sicurezza dei dati aziendali, la risposta deve essere abbracciare una nuova cultura della sicurezza IT che evolva di conseguenza.
Backup - Disaster Recovery

KEY WORD

#RESILIENTE
resilièntе agg. [dal lat. resiliens - entis, part. pres. di resilire «rimbalzare»]. 1. Dotato di resilienza, che presenta maggiore o minore resilienza: materiali r.; pavimenti, rivestimenti resilienti. 2. Per estens., riferito a persona, che oppone resistenza, che si difende con forza: Schiacciata sotto il peso del corpo mascolino, Line si torceva, avversario tenace e r., per eccitarlo e sfidarlo (P. Levi).

#WORM
Acronimo: Write Once Read Many. Dal punto di vista digitale, standard de facto per dispositivi quali Tape (nastri magnetici) che non possono essere sovrascritti o cancellati una volta che siano stati scritti la prima volta.

Nel prossimo **WhitePaper I 03** introdurremo il concetto di Immutabilità.
In questo documento proporremo le soluzioni studiate per i nostri clienti.

sommario
IMMUTABILITA'

ADVNET ADVANCED THINKING

Advnet s.r.l.
Via Marco Corner, 19/21
36016 Thiene (VI) Italy

Tel 0445 371093
Fax 0445 371094

www.advnet.it
sales@advnet.it