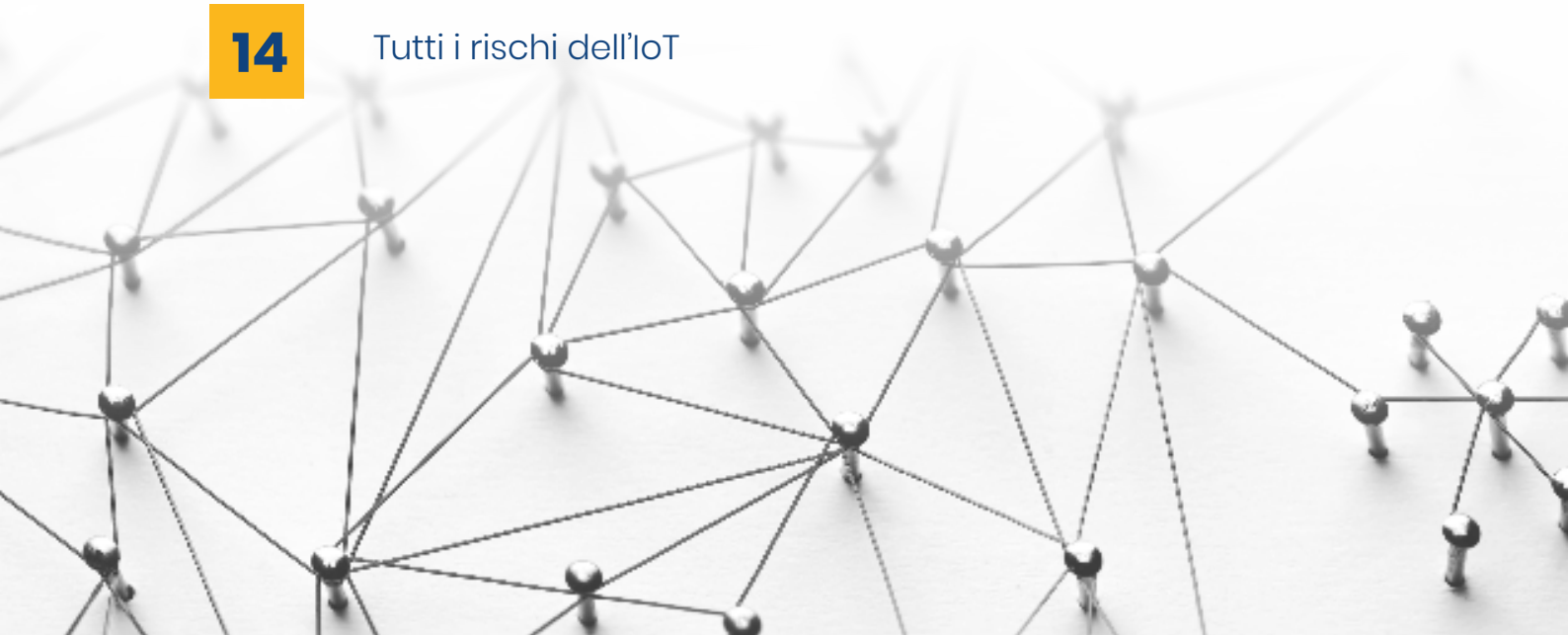
WHITE PAPER

ZERO TRUST SECURITY:

Come essere già pronti ai cyber attacchi che ancora non esistono.

LumIT
A DGS COMPANY

INDICE

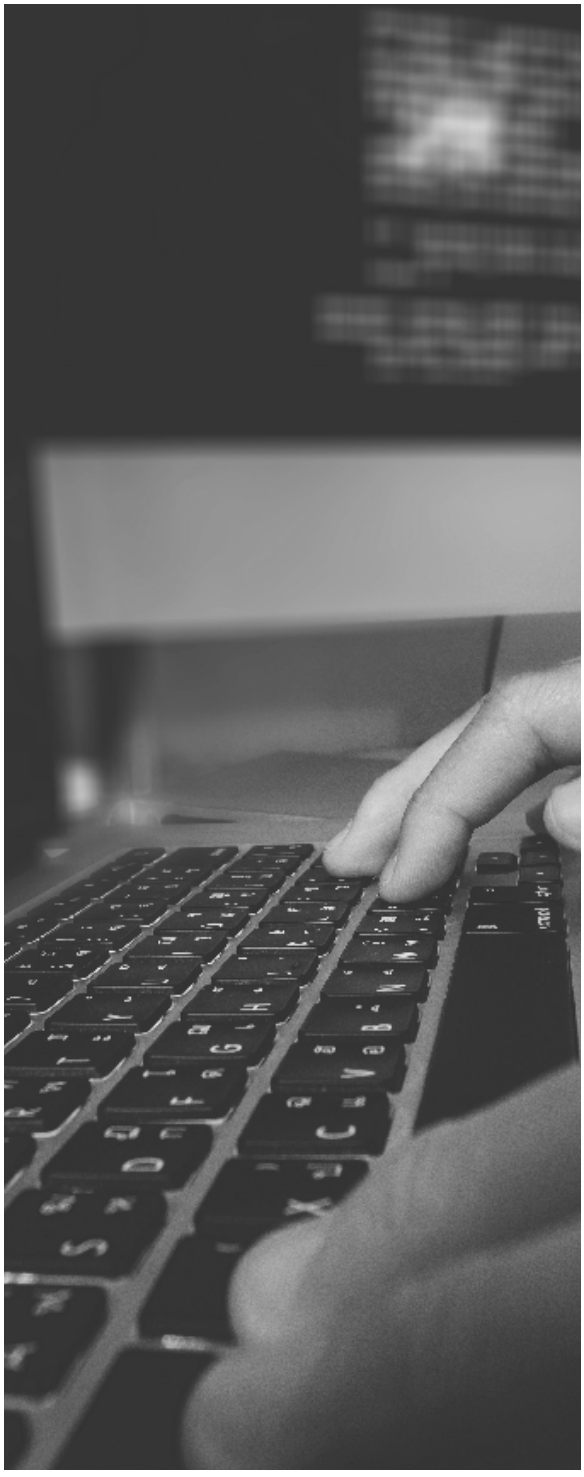


INTRODUZIONE

Chi lavora nella sicurezza informatica sa di muoversi in un mondo in continua evoluzione, in cui le strategie per difendere gli asset aziendali dai cyber attacchi devono essere adeguate e rimodulate di continuo per fare fronte alle nuove minacce. Periodicamente, però, il settore attraversa dei passaggi evolutivi più “bruschi”, che comportano un cambio di prospettiva complessiva. L’approccio Zero Trust Security rappresenta uno di questi.

ADDIO AL PERIMETRO

Il fattore fondamentale che ha portato alla necessità di modificare le **strategie di cyber security** in direzione della filosofia Zero Trust può essere identificato con il **processo di digitalizzazione** che sta interessando aziende, enti pubblici e organizzazioni a tutti i livelli e che **introduce una nuova declinazione del concetto stesso di reti IT**. La conseguenza di questo processo di innovazione è riassumibile nella evaporazione del concetto di "perimetro", sul quale erano basate le tradizionali strategie di cyber security. Se in passato era possibile distinguere tra un "dentro" e un "fuori", nel panorama attuale il network aziendale ha raggiunto un'estensione e un'articolazione tali da rendere impossibile una simile distinzione. L'introduzione dei **servizi cloud**, l'adozione di infrastrutture basate sul concetto di **Software Defined Network** (SDN) e l'adozione sempre più generalizzata di forme di lavoro "agile" da remoto e in mobilità, hanno allargato i confini della rete aziendale, creando al tempo stesso delle aree grigie in cui i servizi e le risorse dell'impresa sono erogati dall'esterno (nel caso del cloud) o fruiti al di fuori dei confini aziendali.



MINACCE IN CONTINUA EVOLUZIONE

In un panorama sempre più complesso a livello di infrastrutture, i pirati informatici hanno la possibilità di insinuarsi tra le pieghe delle reti aziendali con maggiore facilità. Negli ultimi anni, inoltre, i cyber criminali hanno dimostrato di avere un'incredibile capacità di adattamento e di essere in grado di sfruttare a loro vantaggio qualsiasi opportunità si apra. Oltre a un costante aumento degli attacchi "opportunistici", quelli cioè che **sfruttano le vulnerabilità** che emergono di settimana in settimana, nel mondo della criminalità informatica si sono sviluppate **reti underground** sulla logica del **"malware as a service"**, con sistemi di affiliazione e collaborazioni estremamente strutturate. Nei forum e sui market del Dark Web c'è un continuo scambio di informazioni, strumenti di hacking e risorse che i cyber criminali possono utilizzare per le loro attività. **I cyber criminali cambiano le loro strategie a una velocità folle**, adottando le tecniche più efficaci a seconda degli scenari che si presentano. In definitiva, il contesto di fronte a cui si trovano i responsabili di cyber security è radicalmente diverso rispetto al passato. La chiave, infatti, non è proteggersi dalle minacce esistenti, ma essere in grado di individuare tempestivamente quelle sconosciute.

COM'È CAMBIATO IL RANSOMWARE

Rappresenta la maggiore minaccia per le aziende ed è in costante crescita. Quello dei ransomware è un fenomeno che, a differenza di altre forme di cyber crimine, non è caratterizzato da elementi tecnici ma dalle specificità della tecnica, che **punta sul riscatto** (ransom) come elemento di monetizzazione dell'attacco. Se le prime forme di attacco rivolte alle aziende puntavano a estorcere denaro attraverso la "presa in ostaggio" dei dati attraverso sistemi di crittografia, chiedendo un pagamento per ottenere la chiave di **decodifica dei dati**, la nuova strategia prevede la semplice minaccia di pubblicazione delle informazioni sottratte. Una minaccia che fa leva sia sulla preoccupazione legata a un danno reputazionale (o competitivo) sia sul rischio che la semplice violazione dei dati possa portare a sanzioni ai sensi del **Regolamento Generale sulla Protezione dei Dati** (GDPR) in vigore dal 2018.

ANTIVIRUS IN DIFFICOLTÀ

La **necessità di adeguare le strategie di cyber security** per contrastare gli attacchi dei pirati informatici deriva, oltre che dal mutato quadro generale, anche dalle strategie adottate dai cyber criminali per portare i loro attacchi. A differenza di quanto accadeva passato, in cui il pericolo per le aziende era rappresentato principalmente dai classici malware, oggi la maggior parte dei cyber attacchi sfruttano strumenti di hacking differenti, che spesso possono sfuggire al controllo dei normali software antivirus. Sempre più spesso i pirati informatici si affidano a **tecniche di social engineering** (e in particolare agli attacchi di phishing) per ottenere l'accesso alle reti aziendali, per poi eseguire il cosiddetto "movimento laterale" utilizzando normali strumenti di amministrazione che i software di protezione non identificano come malevoli. Insomma: l'uso di tool normalmente dedicati alla gestione dei sistemi informatici consente ai malintenzionati di "passare sotto i radar" e mettere a segno i loro attacchi con maggiore facilità rispetto a quanto accadrebbe utilizzando veri e propri malware. A peggiorare la situazione concorre poi l'attivismo dei cosiddetti gruppi Advance Persistent Threats (APT), professionisti del cyber spionaggio che agiscono per conto di governi e servizi segreti. I gruppi di questo tipo, oltre che su una elevata professionalità, possono contare su mezzi (tecnologici ed economici) decisamente superiori a quelli a disposizione dei comuni cyber criminali, che gli consentono di utilizzare attacchi che sfruttano vulnerabilità zero-day.

GLI STRUMENTI DI PENETRATION TEST DIVENTANO UN'ARMA A DOPPIO TAGLIO

È uno dei paradossi del mondo della sicurezza, che riguarda strumenti software che, per assurdo, sono stati sviluppati per garantire una maggiore sicurezza dei sistemi. I vari kit dedicati al penetration testing, normalmente usati dagli "**hacker etici**" per mettere alla prova il livello di sicurezza delle reti aziendali, sono oggi un formidabile strumento nelle mani dei pirati informatici, che li utilizzano per aprirsi la strada nelle reti aziendali che vogliono violare.
Il paradosso, ancora una volta, affonda le radici nei **differenti tempi di reazione tra ciò che accade nel mondo della cyber security e nella sua effettiva implementazione nella realtà aziendale**. Software come Mimikatz e altri strumenti abitualmente usati dagli esperti di sicurezza, che dovrebbero essere considerati una sorta di "standard" negli assessment di sicurezza ed essere quindi facilmente rilevati, rappresentano ancora una minaccia.

IL CLOUD CONCENTRA L'ATTENZIONE SULLA GESTIONE DEGLI ACCESSI

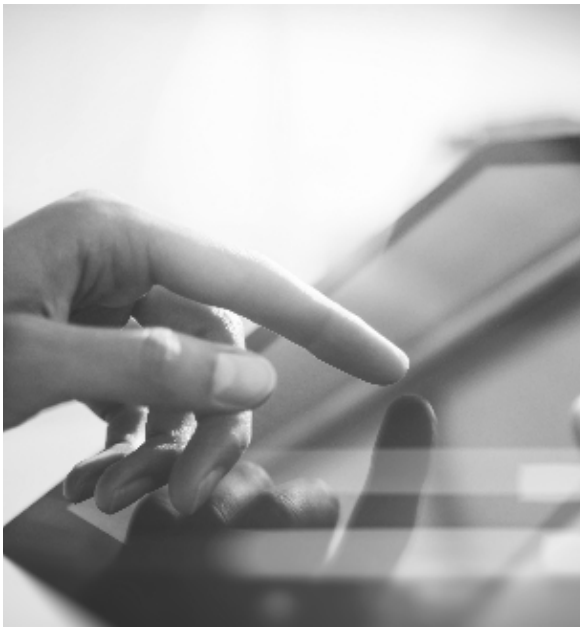
La **migrazione verso le piattaforme cloud**, come accennato, ha modificato radicalmente l'architettura delle infrastrutture IT aziendali, aumentandone il livello di complessità e la superficie di attacco a disposizione dei pirati informatici. La nuova declinazione nell'erogazione dei servizi digitali, però, ha impattato anche sotto un altro profilo. L'implementazione di servizi basati su cloud, infatti, ha "spostato" buona parte della protezione sul controllo degli utenti. La presenza di servizi erogati dall'esterno, così come l'ampliamento dei dispositivi attraverso cui gli impiegati possono accedervi anche in mobilità, **concentrano i layer di sicurezza sulle procedure di accesso**. Un sistema che, se basato solo sull'uso di credenziali tradizionali (username e password), apre la strada ad attacchi basati su tecniche relativamente semplici, che utilizzano strumenti non rilevabili come malware, ma che fanno piuttosto leva su tecniche di ingegneria sociale. Altrettanto rilevante, in questo scenario, è la **gestione dei privilegi**. La definizione di policy accurate, che consentano di limitare il campo d'azione di ogni utente solo a ciò che è necessario, rappresenta in questo senso un elemento fondamentale per impedire eventuali intrusioni.

ATTACCHI DI PHISHING IN COSTANTE AUMENTO

I dati rilevati negli ultimi mesi confermano le tendenze indicate dagli esperti di cyber security, particolarmente per quanto riguarda il fenomeno del phishing. La tecnica utilizzata dai pirati informatici **sfrutta** di solito **semplici email** composte in modo da apparire come provenienti da soggetti legittimi. L'obiettivo è quello di attirare le potenziali vittime su siti Web del tutto simili a quelli originali (ma in realtà sotto il controllo dei cyber criminali) in cui ai visitatori viene richiesto l'inserimento delle credenziali di accesso. In Italia, nel corso del 2020, il phishing **ha subito un aumento del 250%** (i dati si riferiscono anche agli attacchi rivolti ai privati) e, **a livello aziendale, rappresenta più del 60% degli attacchi** andati a segno nei confronti delle aziende (dati Clusit relativi al primo semestre 2020).

LA NECESSITÀ DI UN APPROCCIO ZERO TRUST

Nel quadro descritto, le **strategie di cyber security** richiedono un cambio di prospettiva rispetto all'approccio tradizionale basato sulla logica del perimetro e di una attribuzione di "affidabilità" basata su parametri che non sono più adeguati al contesto attuale. La **filosofia Zero Trust** parte da una semplice premessa: nessun dispositivo o processo può essere considerato affidabile. La prima regola è, di conseguenza, **diffidare di tutto e di tutti**. A partire, per esempio, dagli accessi. In una logica Zero Trust, il processo di autenticazione ai servizi aziendali viene sottoposto non solo a un "irrobustimento" declinato attraverso l'**implementazione di sistemi multi-fattore** (token, OTP e rilevamenti biometrici), ma anche a un monitoraggio continuo che utilizza **strumenti di controllo per verificare la legittimità degli accessi**. In questo senso, i parametri di controllo prevedono l'identificazione del dispositivo utilizzato, la geolocalizzazione e l'analisi a livello di **user behaviour**, come il raffronto con gli abituali orari di accesso.



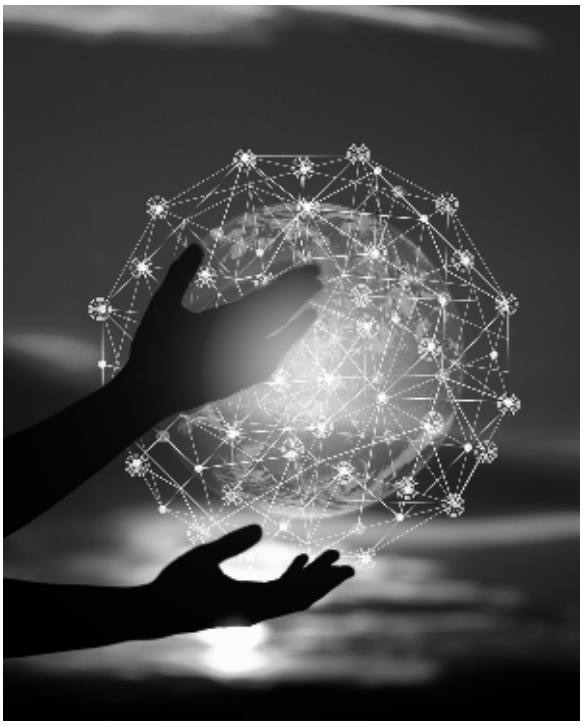
IL FATTORE UMANO

La nuova declinazione della cyber security, al di là dell'evoluzione tecnologica, investe la gestione complessiva dell'infrastruttura IT. A rivestire un ruolo fondamentale in questa prospettiva è il fattore umano, cioè **la capacità degli impiegati di utilizzare gli strumenti a loro disposizione** adottando tutti quegli accorgimenti e precauzioni che garantiscono un livello adeguato di sicurezza. **L'educazione a una "cultura della cyber security"** sta di conseguenza assumendo un ruolo centrale nelle strategie delle aziende. Un obiettivo, quello dell'**alfabetizzazione in ambito cyber security**, che richiede uno sforzo da parte delle aziende ma che rappresenta un investimento estremamente redditizio. Secondo gli esperti di sicurezza, infatti, l'errore umano sarebbe all'origine dell'80% degli incidenti di sicurezza. Ridurne l'impatto sarebbe estremamente proficuo.

LA SEGMENTAZIONE NELLA STRATEGIA ZERO TRUST

La filosofia Zero Trust non riguarda solo utenti e accessi. La stessa logica è infatti applicabile anche a livello tecnico. La parola chiave, in questo caso, è "segmentazione". Il concetto, nella sua declinazione tradizionale, si riferisce **all'esigenza di separare le diverse aree della rete aziendale per creare una sorta di impermeabilità tra quelle esposte su Internet**, per esempio la parte che ospita i server Web, **e quelle che contengono dati sensibili**, come i database o le risorse critiche. Nell'accezione Zero Trust, la segmentazione acquisisce una maggiore **granularità** e non riguarda più "macro aree" del network, ma i singoli processi a livello di server. Nella pratica, ogni servizio viene isolato dagli altri, in modo da impedire a eventuali intrusi quello che viene comunemente definito movimento laterale.

L'applicazione della "diffidenza a priori" nei confronti di qualsiasi attività interna al network aziendale rappresenta inoltre uno strumento prezioso per intercettare tutte quelle attività apparentemente legittime (come nel caso dell'utilizzo di strumenti di amministrazione o di pentetration test) che potrebbero aggirare i tradizionali controlli antivirus, aumentando le capacità di detection dei sistemi di cyber security anche di fronte a ciò che, normalmente, non verrebbe considerato una minaccia.



TUTTI I RISCHI DELL'IOT

I dispositivi di **Internet of Things** (IoT) **rappresentano oggi un fronte su cui gli esperti di sicurezza informatica stanno concentrando la loro attenzione**. I dispositivi "intelligenti" di questo tipo si collocano infatti in un'area grigia che i **pirati informatici sono in grado di utilizzare per portare attacchi alle reti aziendali** sfruttando una sorta di ambiguità che li caratterizza: troppo semplici per poter ospitare strumenti di controllo come i software antivirus, i device IoT possono comunque accedere alle comunicazioni di rete come il resto degli endpoint e rappresentare di conseguenza il punto di accesso ideale per portare un attacco al network aziendale. **L'applicazione di un approccio Zero Trust in questo ambito permette di mitigare il rischio** legato a una compromissione di quelli che, a tutti gli effetti, rappresentano il vero "anello debole" delle reti.

SE VUOI SAPERNE DI PIÙ

CONTATTACI

VIA MILANESE 20
20099 SESTO SAN GIOVANNI

INFO@LUMIT.IT
SALES@LUMIT.IT

WWW.LUMIT.IT