Remotegrant: Sicurezza Informatica e Protezione dei Dati per le PMI

L’intervento di Valerio Pastore, cofondatore di Cyber Grant, intitolato “Allarme Data Breach: 7 attacchi su 10 in EMEA hanno rubato i tuoi dati. Attenzione anche alle minacce interne!”, tenuto durante il 22° Forum ICT Security, esplora le sfide attuali, tra cui il pregiudizio che porta a minimizzare i rischi di ransomware da parte delle PMI e l’importanza di soluzioni avanzate come Remotegrant per la protezione dei dati. Il relatore fornisce un’analisi dettagliata delle minacce alla sicurezza informatica e delle soluzioni proposte dall’azienda americana con radici italiane, con un focus specifico sulle piccole e medie imprese (PMI).

Il Fattore Umano nella Sicurezza Informatica

Valerio Pastore introduce il concetto dei “**60 secondi”: il tempo medio necessario affinché un virus infetti un dispositivo dopo che l’utente clicca su un link malevolo**. Questo dato sottolinea la criticità del fattore umano nella catena della sicurezza informatica, evidenziando l’urgenza di interventi mirati per affrontare questo punto debole.

Secondo il **Data Breach Investigations Report di Verizon**, **il 68% delle violazioni di dati è causato dall’errore umano**, rendendo evidente la vulnerabilità dell’elemento umano nella sicurezza. Nel 2023, sono stati analizzati oltre 30.000 incidenti di sicurezza, registrando un incremento significativo rispetto all’anno precedente. Inoltre, **il 12% degli attacchi deriva da insider**, ovvero persone interne all’organizzazione con accesso privilegiato, mentre una parte

consistente delle violazioni è collegata a vulnerabilità di fornitori o partner esterni.

Le PMI come Obiettivo dei Cybercriminali

Il 60% delle PMI non si percepisce come bersaglio di minacce cyber, nonostante quasi la metà di esse abbia già subito attacchi ransomware, che , nella grande maggioranza dei casi, avvengono in modo silente, con **un tempo medio di rilevamento di circa 204 giorni nel 2023**. Quando una violazione viene scoperta, i danni sono solitamente già stati inflitti.

L'evoluzione del ransomware ha visto una transizione da attacchi immediatamente distruttivi a strategie subdole e persistenti. Oggi, una volta che un dispositivo è stato infettato, viene installata una "backdoor" per monitorare le attività dell'utente, adattandosi alle abitudini aziendali, come l'uso di servizi cloud per la sincronizzazione dei dati. Questo modus operandi rende gli attacchi difficili da rilevare, poiché i dati vengono sottratti in piccole quantità fino a raggiungere una massa critica che viene poi sfruttata per estorsioni e pubblicazioni nel dark web.

Lavoro Ibrido e Uso dell'Intelligenza Artificiale

Le PMI risultano particolarmente vulnerabili con l'aumento del lavoro ibrido, che ha ampliato notevolmente la superficie di attacco. Si stima che **il 70% dei dipendenti utilizzi il PC aziendale per attività personali**, aumentando esponenzialmente il rischio per la rete aziendale. L'utilizzo di soluzioni cloud e l'adozione imprudente di intelligenza artificiale, come l'inserimento di dati sensibili in strumenti come ChatGPT, espongono ulteriormente le aziende a potenziali violazioni del GDPR e ad altri rischi di sicurezza.

La Carenza di Consapevolezza nelle PMI

Un problema cruciale nelle PMI è la mancanza di consapevolezza e di risorse per la sicurezza informatica. L'assenza di aggiornamenti regolari, l'impiego di sistemi di protezione inadeguati e la carenza di personale qualificato le rendono particolarmente vulnerabili agli attacchi informatici. Le conseguenze possono essere devastanti, includendo danni finanziari diretti, interruzioni operative, perdita di proprietà intellettuale e danni alla reputazione. Il furto di proprietà intellettuale, in particolare, è spesso trascurato, poiché avviene in maniera silenziosa e passa inosservato fino a quando è troppo tardi per intervenire.

Remotegrant: Una Soluzione Avanzata per la Sicurezza

Per rispondere a queste sfide, Cyber Grant ha sviluppato " Remotegrant", una soluzione avanzata per la protezione degli endpoint, con un focus specifico sulla prevenzione delle perdite di dati (Data Loss Prevention, DLP). Remotegrant non è una semplice soluzione DLP; oltre a mitigare il rischio umano, monitora costantemente le applicazioni che potrebbero rappresentare una minaccia. Il sistema è in grado di prevenire copie non autorizzate, controllare l'uso delle applicazioni e mitigare le minacce sia interne che esterne, come phishing e ransomware. Inoltre, Remotegrant è in grado di monitorare applicazioni sviluppate internamente, che potrebbero rappresentare minacce sconosciute, come i virus "zero day".

Zero Trust Application: Una Filosofia di Protezione Completa

Remotegrant adotta una filosofia di sicurezza "Zero Trust Application", fornendo protezione trasparente e avanzata all'interno dell'organizzazione. Questo approccio garantisce che l'accesso ai dati sia consentito solo a soggetti e

applicazioni esplicitamente autorizzati. Pertanto, in assenza di un’autorizzazione chiara e verificabile, l’accesso ai file rimane bloccato, impedendolo sia a software dannosi sia al personale interno non autorizzato. L’architettura di Remotegrant è progettata per operare a livello di sistema operativo, garantendo una protezione profonda contro ogni tentativo di accesso non autorizzato.

Tracciabilità Completa e Controllo Granulare

La tracciabilità completa delle attività sui file rappresenta un ulteriore punto di forza di Remotegrant. Ogni accesso ai dati viene monitorato, consentendo la visibilità sulle operazioni compiute e prevenendo condivisioni non autorizzate senza la necessità di utilizzare la crittografia manuale. Questo assicura la protezione dei dati anche durante l’utilizzo delle applicazioni aziendali più comuni, come Google Mail, Teams o Slack. I file rimangono protetti e non trasferibili attraverso strumenti di comunicazione standard, a meno che non sia espressamente autorizzato.

Remotegrant permette un controllo granulare delle applicazioni, come PowerShell, consentendone l’uso solo per attività specifiche e impedendo l’uso non autorizzato dei dati. Inoltre, supporta ambienti virtuali (VDI) e connessioni remote, garantendo la sicurezza dei dati anche in contesti di lavoro su macchine remote. Ad esempio, un utente può caricare file su una macchina remota per lavorarci, ma non può scaricarli sul dispositivo locale, garantendo così un elevato livello di sicurezza.

Protezione dei CRM e Call Center

La protezione delle informazioni contenute nei CRM rappresenta un’area critica per molte aziende. Remotegrant garantisce che i dati nei CRM web non possano essere scaricati, catturati o manipolati senza autorizzazione, fornendo un livello di sicurezza superiore rispetto all’accesso tramite browser convenzionali. Ad esempio, Remotegrant impedisce la cattura di

screenshot, il download di pagine web e l’accesso in modalità sviluppatore per prevenire la sottrazione di informazioni sensibili.

Questa tecnologia risulta particolarmente utile anche nei call center, dove la protezione delle informazioni dei clienti è fondamentale. Remotegrant impedisce agli operatori di effettuare screenshot o scaricare dati sensibili, garantendo che le informazioni rimangano protette e accessibili solo per scopi autorizzati.

Funzionalità Avanzate per la Protezione delle Connessioni Remote

Un’altra funzionalità avanzata di Remotegrant è la possibilità di nascondere le porte RDP (Remote Desktop Protocol), rendendole invisibili quando non sono in uso, aumentando così la sicurezza delle connessioni remote. Inoltre, Remotegrant include una tecnologia di rilevamento delle minacce che sfrutta 75 antivirus tra i più diffusi a livello mondiale, permettendo di identificare in tempo reale attività di phishing e altre minacce. Questa capacità è cruciale per bloccare rapidamente qualsiasi tentativo di compromissione, soprattutto considerando che bastano “60 secondi” per infettare un dispositivo.

Conclusione

In conclusione, Remotegrant rappresenta una soluzione avanzata di Data Loss Prevention che integra la protezione degli endpoint, il monitoraggio delle applicazioni e la prevenzione delle perdite di dati in un’unica piattaforma completa. L’obiettivo è quello di proteggere le PMI dalle minacce sempre più sofisticate e garantire un ambiente di lavoro sicuro e trasparente.

Profilo Autore

Valerio Pastore è una figura di spicco nel settore della

sicurezza informatica, con una lunga e diversificata carriera, focalizzata ad innovare e rendere accessibili le soluzioni di cybersecurity.

Imprenditore seriale, Valerio è stato consulente per strutture militari e ha ricoperto il ruolo di esperto di crittografia per istituzioni pubbliche. Attualmente, Valerio è il fondatore di Cyber Grant Inc., un'azienda innovativa nel campo della cyber security con sede a Menlo Park, California. La sua missione è sviluppare soluzioni avanzate di sicurezza informatica e renderle accessibili a individui e imprese di tutto il mondo.

Nel 2011 ha fondato BooleBox, una innovativa suite di applicazioni per la protezione dei dati aziendali, che utilizza una crittografia di grado militare per salvaguardare informazioni sensibili. Tra i clienti premium di BooleBox c'è la Commissione Europea e la European Defense Agency.

Valerio, inoltre, è il Managing Partner di Tailor Ventures, una società di venture capital con focus su start up tech.

Come CTO presso VALMAX Software, ha guidato lo sviluppo di soluzioni personalizzate di sicurezza informatica. Nel 2021, ha svolto un ruolo chiave in xbinary, contribuendo a fornire soluzioni basate su blockchain per il segmento di lusso e la transizione verso il Metaverso. Nel 2020, ha co-fondato Convy School, una piattaforma per combattere il bullismo e il cyberbullismo nelle scuole italiane.

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/articoli/remotegrant-sicurezza/