GenData
CUSTODIAMO LA VOSTRA CONOSCENZA

Il primo passo da compiere
per anticipare un attacco informatico,
è imparare a conoscerne
le diverse tecniche di aggressione.

CYBER CRIME

Strategie e strumenti per anticiparlo

CUSTODIAMO LA VOSTRA CONOSCENZA

/ Phishing /
Mail dalla parvenza innocua, progettate per indurre in errore il dipendente e fargli fornire informazioni personali direttamente agli attaccanti. Gli hacker utilizzano l'AI per creare mail altamente personalizzate, in grado di ingannare chiunque.
I pericoli a cui è possibile andare incontro possono essere:
• Furto di informazioni personali
• Iniezione di virus nel computer
• Installazione di spyware o adware per monitorare le azioni dei dipendenti online.

/ Attacchi laterali /
Attraverso innovative tecniche di attacco, un'applicazione consolidata viene educata da un hacker a tenere un comportamento diverso dallo standard, garantendogli una porta di ingresso nell'infrastrutture aziendale

/ Malware /
È un software che può modificare il funzionamento del computer, raccogliere informazioni sensibili o ottenere l'accesso non autorizzato a un sistema informatico.

/ Virus /
La più classica forma di attacco, che ha il semplice obiettivo di arrecare quanto più danno possibile all'azienda vittima.

Entrare nella mente di un hacker per anticipare ogni sua mossa

/ RANSOMWARE /
È un tipo specifico di virus che rende illeggibili i dati sul pc. I criminali informatici richiederanno un riscatto, in cambio dello sblocco. Nessun tradizionale antivirus è in grado di fermarlo, visto che l'operazione di crittazione dei dati, di per sè non è malevola, lo è il fatto che, una volta fatto, non ci verrà fornita la password di decrittazione, cosa che nessun sistema di sicurezza tradizionale è in grado di prevedere. Le forme comuni di ransomware includono Cryptolocker, Cryptowall, TeslaCrypt.

/ ADWARE E SPYWARE /
Induce a installare un programma che acquisisce informazioni come password, informazioni bancarie e altri dati preziosi, senza il consenso dell'utente. Alcune pagine web installano anche spyware sotto forma di "cookie".

Superficie d'attacco? OVUNQUE.

GenData
CUSTODIAMO LA VOSTRA CONOSCENZA

Capire la superficie di attacco aiuta a ridurre l'esposizione al rischio informatico ed è un buon inizio per adottare una difesa proattiva.
Le PMI sono maggiormente esposte ad attacchi di questo tipo: dati recenti mostrano che il 43% degli attacchi informatici è rivolto alle piccole aziende, e solo il 14% è preparato a difendersi.
Le 2 principali superfici d'attacco sono dispositivi e persone.

/ DISPOSITIVI /
Ogni azienda si connette a Internet utilizzando un numero sempre più alto di dispositivi.
Tenendo conto delle minacce informatiche e delle potenziali vulnerabilità nei sistemi operativi e nel software, è facile capire come tali dispositivi possano contribuire all'espansione della superficie di attacco.

/ PERSONE /
L'anello debole della catena della sicurezza digitale è costituito dal personale aziendale. Secondo Gartner, il 95% delle violazioni cloud si verifica a causa di errori umani, come ad esempio errori di configurazione e più del 70% delle violazioni dei dati è attribuibile ad attacchi di social engineering.
Password e autenticazione a più fattori (MFA), non sono una pratica standard all'interno della maggior parte delle aziende. Il 66% degli utenti continua infatti a utilizzare sempre la stessa password.
Ecco perché i criminali informatici riescono ad ottenere l'accesso alle reti attraverso i dipendenti.
Spesso l'hacker sottrae informazioni personali contattando i dipendenti tramite e-mail, spacciandosi ad esempio per un collega o un'organizzazione credibile.

/ Come è possibile individuare i rischi informatici e la superficie di attacco? /

Non solo attraverso l'analisi a posteriori dei dati di un attacco, ma anche avendo la piena visibilità delle correlazioni tra i comportamenti e le app aziendali, al fine di poter avere chiaro dove e come intervenire in anticipo rispetto a un pericolo.

/ Security Gendata: proteggere dati, informazioni e strumenti /

Sistemi per massimizzare la sicurezza della vostra azienda.

/ Autenticazione a più fattori /

L'autenticazione a più fattori (MFA) è l'unico strumento che può garantire l'effettiva identità delle persone al momento del login nelle applicazioni, attraverso una notifica sul cellulare degli utenti, sarà possibile autenticarsi con un singolo comando, a tutte le app federate con il sistema, raggiungendo un duplice vantaggio: nessuna password da ricordare, ma solo l'autenticazione attraverso lo strumento nativo del telefono (face id, impronta digitale, etc...); un singolo accesso per tutte le app.

Servizio di autenticazione

Gestione del cloud

App mobile

Token hardware

/ Protezione in movimento / Protezione DNS

Semplifica la difesa della rete aziendale identificando in modo proattivo le richieste DNS legate a contenuti dannosi, il software impedisce che i clic rischiosi diventino importanti incidenti di sicurezza. Quando un utente fa clic su un collegamento o immette un indirizzo web nel proprio browser, la soluzione monitora e correla il traffico DNS, identificando e bloccando le connessioni ai domini di proprietà dei malintenzionati.

/ PrivacyLab GDPR /

PrivacyLab GDPR è il software in cloud che permette di gestire quotidianamente tutti gli adempimenti previsti dal Regolamento Europeo 16/679 sulla privacy ed evitare le sanzioni del Garante.
Verifica la sicurezza dei dati personali trattati in azienda, produce tutta la documentazione necessaria (anche in altre lingue), monitora l'intero processo del trattamento dei dati.
PrivacyLab GDPR è certificato secondo i più alti standard di qualità e assicurato a prova di errore.
Analizza la Compliance aziendale, guidando le aziende attraverso la valutazione, la generazione e la gestione di tutta la documentazione necessaria e di tutti gli adempimenti comprese le verifiche organizzative (e l'eventuale formazione).

/ Microsoft Backup365 /

Tutti i dati sotto controllo in 1 soluzione semplice e sicura.
L'eventuale perdita di dati aziendali emerge quasi sempre quando ormai è troppo tardi.
Evitare questi spiacevoli inconvenienti è possibile grazie a una soluzione di backup in grado di offrire l'accesso e controllo completo ai dati di Office 365.

/ Perché è fondamentale avere una soluzione di backup per Microsoft 365? /

Il perché è semplice: Microsoft è responsabile unicamente della manutenzione delle infrastrutture e la disponibilità dell'applicazione.
La protezione dei dati di Microsoft Office 365 è invece una responsabilità completamente a carico delle aziende.

GenData

CUSTODIAMO LA VOSTRA CONOSCENZA

Gendata

CUSTODIAMO LA VOSTRA CONOSCENZA

/ Gensecurity /

Racchiude una serie di applicazioni, selezionate dai tecnici Gendata, per garantire il raggiungimento dei massimi standard di sicurezza aziendale, intesa sia come protezione da attacchi mirati, sia come analisi proattiva dei comportamenti che potrebbero minare l'infrastruttura della vostra azienda.

/ Gensecurity Telemetric Console (GTC) /

Un vero motore di correlazione di eventi, declinato sul mondo degli endpoint, indispensabile per comprendere tutte le dinamiche di interazione tra i diversi applicativi aziendali; in sostanza una vera e propria radiografia della vostra infrastruttura, utile a evidenziare i punti deboli e le consuetudini dei dipendenti che possono portare a falle nelle tradizionali piattaforme di sicurezza, che verranno enormemente potenziate da questo approccio.

/ Gensecurity Zero Trust (GZT) /

Combinando la raccolta telemetrica con la storicità di analisi dei nostri partner tecnologici, GZT riunisce le capacità di un normale antivirus con le funzionalità di sicurezza più avanzate (EDR). Inoltre grazie alla funzionalità inclusa di Threat Hunting, GZT è in grado di proteggere anche da attacchi laterali (il vettore più frequente nell'ultimo semestre) oltre a garantire la completa protezione fin dal momento in cui la minaccia viene creata (zero trust).

/ Windows Full Patch Management /

Gestisce aggiornamenti e patch nel mondo windows, sia a livello di applicativi, sia a livello di sistema operativo. Sulla base delle informazioni raccolte da GTC, il sistema è in grado di fornire informazioni relative non solo allo status delle patch ma anche sui software non più supportati o in fase di EOL, eliminando quindi una grossa criticità a livello endpoint.

/ Gensecurity Full Disk Encryption /

Sfrutta la tecnologia BitLocker, collaudata e affidabile, per crittografare e decrittografare i dischi senza impatto sugli utenti finali, fornendo maggiore controllo e una gestione centralizzata delle chiavi di crittografia, che vengono archiviate centralmente.

CUSTODIAMO LA VOSTRA CONOSCENZA

Perché scegliere Gendata

Il team Gendata vi aiuterà a eliminare i rischi per la vostra azienda e a raggiungere una posizione di sicurezza più forte, costruendo un programma di salvaguardia della vostra attività, solido e duraturo.

Il nostro compito è trasformare i problemi in soluzioni e le aspirazioni in realtà, attraverso servizi di consulenza studiati sulle vostre reali necessità, consigliandovi le migliori risorse presenti sul mercato.

FORLÌ | Via G. Spadolini, 31 | 47122
BOLOGNA | Via E. Mattei, 102 | 40138

+39 0543 752374
+ 39 051 19936408

info@gendata.it | gendata@pec.it
P.I. 04083330409 | REA FO – 328974