COMUNICATO STAMPA

#NewsANRA | febbraio 2023

Cyberwar, urgente una seria politica di security patch management per garantire la sicurezza dei dati aziendali

Una politica di security patch management mantiene sistemi e applicazioni al sicuro dal dilagante cyber crime

Milano - Il mondo digitale ha reso le aziende vulnerabili a minacce informatiche come malware, attacchi ransomware e furto di dati sensibili.

In questi giorni l'Agenzia per la Cybersicurezza Nazionale ha allertato diversi soggetti i cui sistemi risultano esposti e dunque vulnerabili agli attacchi, in particolare ha segnalato che alcuni criminali informatici hanno avviato delle attività di scansione alla ricerca di server virtuali VMware ESXi, vulnerabili ad un bug di sicurezza noto come CVE-2021-21974.

Possiamo comprendere quanto proteggere il perimetro aziendale digitale diventi sempre più importante per garantire la sicurezza dei dati aziendali e prevenire attacchi informatici.

Anche il Rapporto Clusit nella sua edizione di ottobre 2022 ci racconta che, tra le tecniche di attacco utilizzate dai cyber criminali, lo sfruttamento di vulnerabilità rappresenta circa l'11% del totale.

Uno dei modi più efficaci per proteggere il perimetro aziendale digitale è attraverso una politica di ***security patch management***. Questa politica prevede la regolare applicazione di patch di sicurezza su tutti i sistemi, le applicazioni e i dispositivi della rete aziendale. Queste patch correggono vulnerabilità di sicurezza note che potrebbero essere sfruttate da cyber criminali per accedere alle informazioni sensibili dell'azienda.
Inoltre, una politica di security patch management aiuta a mantenere i sistemi e le applicazioni aggiornati e al sicuro da minacce informatiche emergenti. Ciò significa che i cyber criminali non avranno accesso alle vulnerabilità che possono essere sfruttate per entrare nella rete aziendale.

Un'altra motivazione importante per proteggere il perimetro aziendale digitale è preservare la reputazione dell'impresa. Un attacco informatico può avere conseguenze negative sulla reputazione dell'azienda e danneggiare la sua immagine di fronte ai clienti, ai partner commerciali e alla comunità. Una politica di security patch management aiuta a prevenire questi attacchi, preservando così la reputazione.

Infine, una politica di security patch management aiuta a minimizzare la superficie di attacco esposta ai cyber criminali. Con una maggiore sicurezza dei sistemi e delle applicazioni, i cyber criminali avranno meno opportunità di entrare nella rete aziendale e rubare i dati sensibili. Ciò riduce il rischio di perdita finanziaria e garantisce che i dati aziendali siano al sicuro.

In sintesi, proteggere il perimetro aziendale digitale con una politica di security patch management è importante per garantire la sicurezza dei dati aziendali, preservare la reputazione aziendale e offrire minor superficie di attacco ai cyber criminali.

Giovanni Finetto – Socio ANRA

06 febbraio 2023

COMUNICATO STAMPA

ANRA | Dal 1972 raggruppa i Risk Manager e i Responsabili delle Assicurazioni Aziendali. ANRA è l'Associazione dei Risk Manager e Responsabili Assicurazioni Aziendali, si pone come obiettivi:

- promuovere lo scambio tra i Soci di esperienze e informazioni in materia di gestione di rischi aziendali, management d'impresa, politiche assicurative, definizione e gestione dei contratti di assicurazione;
- contribuire al progresso ed alla divulgazione delle tecniche di gestione dei rischi, mediante l'organizzazione di corsi di formazione, di aggiornamento professionale e di ogni altra iniziativa appropriata operando anche con Associazioni del settore, sia italiane sia estere, Istituti Assicuratori, Enti, Università, Autorità Pubbliche competenti, brokers e periti, assicuratori e riassicuratori.

ANRA è consapevole delle sfide e delle opportunità che il mercato impone e sa che per affrontarle occorrono decisioni rapide e vincenti. Perseguire l'efficacia e l'efficienza aziendale significa superare le sfide ed individuare le opportunità. È in quest'ottica che l'Associazione ha deciso l'istituzione prima, il conseguimento ed il mantenimento poi di un sistema qualità conforme agli standard internazionali ISO 9001 che permetta di garantire una maggior efficienza interna ed una migliore predisposizione a dimostrare la propria capacità di fornire prodotti che soddisfano i requisiti del cliente e i requisiti cogenti applicabili, ad accrescere la soddisfazione del cliente, affrontare rischi e opportunità associati al suo contesto e ai suoi obiettivi. Il documento Politica della Qualità è disponibile in allegato.

Le attività tramite cui ANRA persegue i propri obiettivi sono:

FORMAZIONE Per contribuire al progresso e alla divulgazione della cultura del Risk e Insurance Management, ANRA organizza corsi di formazione e aggiornamento professionale finalizzati alla preparazione di figure aziendali specifiche. Tutta la formazione ANRA è certificata ISO 9001 e Ferma Rimap, è riconosciuta dall'Ivass e dall'Ordine degli Attuari.

INFORMAZIONE E CULTURA Attraverso il portale www.anra.it e la rivista bimestrale RM News, ANRA garantisce informazione aggiornata, costante e qualificata, per contribuire alla diffusione della cultura d'impresa attraverso la gestione del rischio e delle assicurazioni.

NETWORKING ANRA può contare sul supporto di enti universitari, società di consulenza, analisi e ricerca, compagnie assicurative, broker, società di servizi nell'ambito del rischio d'impresa. Con le loro competenze specifiche, tutti questi attori portano valore aggiunto ai membri dell'Associazione e alle loro imprese.

VITA ASSOCIATIVA I Soci ANRA possono contare su un ricco calendario di convegni e workshop, corsi di formazione, supporto e consulenza, ricerche e contenuti esclusivi, convenzioni e servizi professionali.

Per conoscere tutte le iniziative ed essere aggiornati in tempo reale: **anra.it**

Ufficio Stampa: Parole & Dintorni S.r.l.

Francesco Maria Gallo | Public Affairs Manager
Cell +39 3738541868 | fmgallo@paroleedintorni.it | paroleedintorni.it