EUROPEAN
RENTAL
ASSOCIATION

RIEPILOGO ESECUTIVO

Guida ERA alle leading practice di sicurezza informatica nel settore del noleggio di attrezzature

Sicurezza informatica – la tua azienda è pronta per la sfida?

Una delle principali minacce per il settore del noleggio delle attrezzature è rappresentata dalla vulnerabilità delle nostre aziende agli impatti della sicurezza informatica. Nel 2021 manca ancora una roadmap consolidata nel nostro settore, in cui un'azienda di noleggio di attrezzature può valutare la propria posizione in relazione alla sicurezza informatica e identificare le leading practice cui aspirare. Scopo di questa Guida è quello di definire l'ambito di intervento a livello aziendale in materia di sicurezza informatica, identificare gli elementi chiave di una strategia di successo, compresi i fattori speciali che possono influire sulle società di noleggio, e delineare le leading practice oggi adottate dai leader del nostro settore. La presente Guida è stata redatta con l'inestimabile supporto e contributo delle aziende aderenti all'ERA.

La minaccia della sicurezza informatica oggi e l'"invito all'azione"

Questa Guida illustra come il settore del noleggio di attrezzature in tutta Europa si trovi ad affrontare una sfida senza precedenti causata dalle minacce derivanti dalle vulnerabilità e dalle esposizioni delle tecnologie dell'informazione nel nostro settore, e in particolare dalle richieste sempre più esigenti dei nostri clienti in materia di protezione informatica. Il settore si trova in un processo di consolidamento, con le aziende più piccole che si fondono con altre per raggiungere gli obiettivi, e con le aziende più grandi che acquisiscono quelle più piccole per entrare in nuovi mercati e consolidare o conquistare la quota di mercato. Il settore del noleggio di attrezzature sta abbracciando la "digitalizzazione". Una maggiore presenza online implica maggiori minacce informatiche. Le attrezzature da noleggio stanno diventando sempre più intelligenti e connesse alle reti che possono costituire il canale di attacco. Le società di noleggio di attrezzature che hanno subito un grave incidente ritengono di aver messo a rischio elevato la loro attività, la loro reputazione e soprattutto i loro clienti e stakeholder. La legislazione dell'UE se ne sta occupando in maniera sempre più massiccia e la Guida indica gli ultimi sviluppi della direttiva UE NIS (Sicurezza delle reti e dei sistemi informativi). Il settore ha ora bisogno di una collaborazione costante tra le aziende europee per studiare le migliori prassi in materia di sicurezza informatica, minacce comuni e problemi che tutte le organizzazioni devono affrontare.

Budget e investimenti per la sicurezza informatica

Questa Guida illustra gli investimenti per una corretta sicurezza informatica e i relativi costi. Presenta una scala degli investimenti e la "maturità" indicante l'investimento iniziale necessario per mettere in essere le basi. Una buona sicurezza informatica richiede investimenti significativi e deve essere rinnovata ogni anno. Gli investimenti diretti nella sicurezza informatica in tutti i settori ammontano a circa il 5% della spesa IT, con una spesa maggiore all'inizio. I leader del settore dimostrano, inoltre, che l'investimento più consistente riguarda i costi indiretti e intangibili di "progettazione", gestione e integrazione della sicurezza in tutto ciò che fanno, il che potrebbe in ultima analisi essere superiore ai costi diretti.

Roadmap delle leading practice e "Lista di controllo"

L'attenzione per gli interventi in materia di sicurezza informatica è spesso focalizzata sulla tecnologia e sui sistemi, tuttavia la causa principale di molti rischi va ricercata nel comportamento umano, nella robustezza dei processi e nel monitoraggio, nella segnalazione e nella risposta all'interno dell'azienda. Secondo i leader in questo campo del noleggio di attrezzature, un'organizzazione deve prendere in considerazione una strategia a livello aziendale atta a garantire che vengano considerate tutte le aree di vulnerabilità. Rischi, portata delle operazioni e lacune sono differenti per ciascuna organizzazione. Tuttavia, i leader ritengono che una lista di controllo per un quadro completo possa essere riassunta in quattro Elementi di Competenza che riguardano Processo, Persone, Tecnologia e Infrastruttura. Pertanto, questa Guida li analizza e presenta i requisiti di competenza fondamentali in ciascuno dei tre livelli: "livello base", "maturazione" e "leader". È inclusa una lista di controllo che, come ausilio per la pianificazione e riduzione dei rischi, collega la valutazione dei rischi e delle vulnerabilità essenziali ai livelli di maturità attuali dell'azienda.

"S*i ottiene ciò che si misura…*" I leader segnalano l'importanza di garantire che le aree chiave delle prestazioni che influiscono sullo stato della sicurezza informatica siano misurate con Indicatori Chiave delle Prestazioni (KPI). La Roadmap della guida indica poi le misure tipiche e i sistemi di misurazione delle prestazioni attualmente in uso presso le aziende leader per ciascuno degli elementi.

Illustrazione delle leading practice

Questa Guida illustra quindi alcune delle leading practice attualmente in uso relativamente ai quattro elementi di competenza. I leader sottolineano che, sebbene un piano di sicurezza esaustivo costituisca una parte essenziale di una strategia globale, il primissimo passo non debba essere un piano onnicomprensivo: in genere un piano completo può arrivare nelle fasi di maturità. Le caratteristiche principali includono:

- **Processo**: I leader sottolineano che, nelle prime fasi, è più importante adottare misure atte ad identificare ogni possibile area ad alto rischio nell'azienda e stabilire la priorità delle azioni per tamponarne o correggerne le vulnerabilità. Una scansione completa dei rischi in ciascuna delle aree di base di questa guida può rappresentare un buon punto di partenza. Nell'esaminare le aree ad alto rischio, si possono verificare le aree a medio rischio. È importante sottolineare che la ricerca indica che, per arrivare a coprire tutte le aree a rischio significativo partendo da un livello base, può essere necessario un processo della durata da tre a cinque anni che richiede investimenti sostenuti e materiali. I leader puntano a un tipo di percorso di base, migliore, del tipo più idoneo per poi arrivare a una sicurezza adatta allo scopo che può utilizzare accreditamenti formali come pietre miliari o essere personalizzata in azienda e seguire gli stessi principi. Vengono delineati alcuni quadri internazionali in uso.

- **Persone:** *La sicurezza informatica non è una "cosa IT"…* La Gestione delle Risorse Umane (HR) ha un ruolo importante nella difesa della sicurezza informatica. L'ambito di intervento e di supporto delle risorse umane nelle società leader è esteso a tutta l'azienda attraverso la progettazione e lo sviluppo di politiche e procedure (compresi il GDPR e i protocolli di protezione dei dati), la loro comunicazione a tutto il personale, l'adattamento dei termini e delle condizioni dei dipendenti e le descrizioni dei ruoli per includere le responsabilità in materia di dati e sicurezza, nonché la consapevolezza e la formazione sui fondamentali della sicurezza informatica e l'analisi delle esigenze di formazione per i ruoli di prima linea e per il personale di sicurezza specifico. I mezzi di comunicazione, quali newsletter o bollettini su social media, sono essenziali per trasmettere le ultime tendenze o minacce in tutta l'azienda.

- **Tecnologia:** Gli strumenti informatici sono in continuo e rapido sviluppo e forniscono un potente mezzo di difesa informatica per l'"allerta precoce" e l'intercettazione delle minacce. Il monitoraggio delle minacce e dello stato di salute è supportato dalla tecnologia con sistemi avanzati come "Splunk" e "MS Azure Sentinel" illustrati in uso. La creazione di un "SOC" (Centro di Operazioni di Sicurezza) è essenziale per ottenere il massimo dalla potenza dei sistemi automatizzati. I leader possono gestire un SOC interno, spesso integrato da centri di terze parti che possono offrire copertura di supporto 24x7 e servizi avanzati di monitoraggio e gestione.

- **Infrastruttura:** *"Se, nonostante tutte le migliori misure di prevenzione, dovesse accadere il peggio è necessario essere pronti con un piano di gestione degli incidenti".* Gli attacchi possono presentarsi in molte forme, ma uno dei tipi più gravi può essere un "attacco ransomware". In una situazione di negazione dei sistemi, è necessaria una risposta di emergenza immediata, ma è necessario mettere in atto un processo per valutare la situazione e analizzarne le priorità mediante "triage". Questa guida illustra le modalità di analisi e di risposta dei leader e fornisce un modello di "prime 48", che può aiutare a pianificare il periodo di gestione della crisi subito dopo un evento di negazione dei sistemi o un'altra grave minaccia di avaria.

Prepararsi a un futuro sicuro

La corsa verso una buona sicurezza IT non finirà mai ma, per restare in testa, i leader sottolineano che le società di noleggio di attrezzature devono:

1. *Conoscere le risorse, i punti di forza e le vulnerabilità*

2. *Eseguire la valutazione dei rischi*
3. *Pianificare e investire in modo appropriato*
4. *Essere pronte nel caso in cui accada il peggio*
5. *Aggiornarsi e migliorarsi continuamente*

La “guida ERA alle leading practice di sicurezza informatica” mira ad aiutare le società di noleggio di attrezzature di ogni tipo e dimensione a pianificare, sviluppare o migliorare continuamente la loro sicurezza informatica.