Suggerimenti: La protezione ransomware nell'era del lavoro flessibile

kaspersky BRING ON THE FUTURE

Il ransomware rimane una minaccia sempre più presente per qualsiasi organizzazione. Le stime suggeriscono che il 15,45% di tutti gli utenti Internet ha subito almeno un attacco basato sul malware nel corso del 2021[1]. Di conseguenza, la sicurezza informatica è una priorità strategica sempre più importante per le aziende.

Il rischio di infezione da ransomware è aumentato negli ultimi anni, in particolare a causa dell'aumento dell'adozione dello smart working reso necessario dalle misure di controllo durante la pandemia. Lo studio suggerisce che la corsa al lavoro a distanza ha comportato una riduzione della supervisione per la maggior parte delle organizzazioni o un allentamento dei consueti protocolli di sicurezza.

Quando si ha a che fare con il ransomware, l'elemento cruciale è il ripristino dell'accesso ai dati criptati il più rapidamente possibile. Tuttavia, vale la pena ricordare che i cybercriminali spesso esfiltrano i file per ricattare ulteriormente gli utenti, chiedendo pagamenti aggiuntivi per evitare che le informazioni sensibili vengano divulgate.

Un numero inferiore di aziende ha distribuito strumenti di sicurezza di rete (meno 5%) o di monitoraggio degli utenti finali (meno 6%) nel corso del 2021[2]. Senza un monitoraggio e una sicurezza efficaci degli endpoint, il rischio di diventare vittima del ransomware aumenta notevolmente.

Gli endpoint sono sempre stati un anello debole nella sicurezza aziendale, spesso proprio le superfici di attacco più accessibili per gli hacker. Ma con lo smart working questi endpoint sono stati trasferiti **all'esterno** del perimetro di rete, rendendo ancora più difficile la gestione e la mitigazione della sicurezza. L'aumento degli endpoint consente agli autori degli attacchi di scegliere tra una gamma più ampia di potenziali bersagli, aumentando ulteriormente le possibilità di successo.

Per prevenire un'importante epidemia di ransomware, è necessario implementare una strategia ransomware efficace suddivisa in più livelli. Poiché il lavoro a distanza sta diventando una costante delle operazioni, le organizzazioni devono perfezionare e rafforzare gli strumenti di protezione degli endpoint, soprattutto in relazione al modo in cui rilevano e bloccano le infezioni ransomware.

Questa guida offre suggerimenti pratici, aiutandovi a valutare il vostro grado di protezione dal ransomware nel perimetro di rete e le aree di miglioramento delle difese, tra cui:

- **1. Rilevamento del ransomware negli endpoint**
- **2. Configurazione degli endpoint**
- **3. Configurazioni di backup**
- **4. Alleggerire le operazioni**
- **5. Formazione per l'utente finale**
- **6. Pianificazione della risposta agli incidenti**

[1]Kaspersky Security Bulletin 2021. Statistiche – Kaspersky –https://securelist.com/kaspersky-security-bulletin-2021-statistics/105205/

[2]Cyber Security Breaches Survey 2021 – UK Department for Digital, Culture, Media & Sport – https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/cyber-security-breaches-survey-2021

1. Rilevamento del ransomware negli endpoint

È estremamente importante fermare il ransomware prima che possa diffondersi. Quando un'infezione viene identificata e bloccata rapidamente, i danni e le interruzioni che potrà causare sono inferiori.

Generalmente l'organizzazione può intercettare un malware inviato direttamente tramite e-mail ai dipendenti al livello del server di posta. Tuttavia, i dipendenti possono anche essere indotti a scaricare file eseguibili esterni con un messaggio di spear phishing creato ad hoc.

Il rilevamento del ransomware può essere migliorato bloccando i file eseguibili sospetti al livello dell'endpoint:

- **Distribuite un robusto toolkit anti-malware per identificare e rimuovere i file eseguibili sospetti prima che possano criptare i file sensibili.**
- **Utilizzate le funzionalità di machine learning degli strumenti EDR (Endpoint Detection and Response) per identificare e bloccare automaticamente le attività sospette del sistema.**
- **Prendete in considerazione l'adozione di una soluzione MDR (Managed Detection and Response) per automatizzare e accelerare le procedure di mitigazione del ransomware.**

La distribuzione di questi strumenti aiuterà a contenere un'infezione, impedendo che si diffonda in altri archivi file e sistemi.

È importante sottolineare che organi federali ed enti governativi stanno assumendo una posizione più netta rispetto alla risposta delle vittime alle infezioni da ransomware. Nel 2019 l'FBI Internet Crime Complaint Center (IC3) ha esortato le aziende a non pagare riscatti[3].

Anche Kaspersky la pensa allo stesso modo: "Non pagate. Ogni volta che si paga un riscatto si contribuisce finanziariamente allo sviluppo del malware e si dà ai cybercriminali la conferma che il loro modello è redditizio. Inoltre, il pagamento non assicura la risoluzione del problema: potreste comunque non riavere indietro nulla."[4]

L'ufficio federale tedesco per la sicurezza delle informazioni (BSI) suggerisce: "La migliore protezione contro le richieste di riscatto da parte dei cybercriminali è l'applicazione coerente delle misure di sicurezza IT".[5]

Grazie a questo comportamento si riescono a mantenere misure di protezione degli endpoint simili **sia all'esterno** che all'interno del perimetro di rete. In questo caso, si tratta di strumenti EDR intelligenti e anti-malware affidabili in grado di rilevare in modo automatico l'attività tipica del ransomware.

2. Configurazione degli endpoint

La configurazione degli endpoint aiuterà anche a ridurre il potenziale effetto di un'infezione ransomware. Per i dispositivi aziendali:

- Utilizzando elenchi delle directory consentite per le applicazioni avrete la certezza che gli utenti eseguano soltanto software autorizzato. Con le giuste restrizioni, i dipendenti non potranno installare applicazioni, riducendo la possibilità di eseguire file infetti.
- Assicuratevi che gli strumenti di protezione degli endpoint e gli altri software installati siano impostati per l'aggiornamento automatico, in modo da bloccare le nuove minacce e chiudere le potenziali falle prima che vengano sfruttate[6].

Le best practice per la sicurezza suggeriscono di applicare gli aggiornamenti software entro 14 giorni dal rilascio. Purtroppo, solo il 43% delle aziende raggiunge questo obiettivo[7]. Questo accorgimento, relativamente facile da implementare, rappresenta uno strumento significativo per prevenire la diffusione del ransomware.

[3] High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations – FBI Internet Crime Complaint Center – https://www.ic3.gov/Media/Y2019/PSA191002

[4] Cinque consigli per proteggervi dai ransomware – Kaspersky – https://www.kaspersky.it/blog/ransomware-five-tips/25400/

[5] Ibid.

[6] Ransomware world in 2021: who, how and why – Kaspersky – https://securelist.com/ransomware-world-in-2021/102169/

[7] Cyber Security Breaches Survey 2021 – UK Department for Digital, Culture, Media & Sport – https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/cyber-security-breaches-survey-2021

Gli endpoint BYOD rappresentano un'ulteriore sfida perché la vostra organizzazione può esercitare solo un controllo limitato sul dispositivo. In questo modello operativo sono disponibili alcune opzioni:

- Incoraggiare i dipendenti a installare uno strumento anti-malware approvato in ogni singolo dispositivo. Fornire questo software gratuitamente è un buon incentivo in quanto consentirà di proteggere non solo i dati personali del dipendente, ma anche le risorse aziendali.
- Inserire nella sandbox dati e applicazioni aziendali per separarli dalle applicazioni personali. Se un dipendente accede al malware utilizzando applicazioni personali, la sandbox offre un certo livello di tutela contro la diffusione.

In definitiva, la protezione dei dispositivi personali degli utenti sarà un compromesso in cui si accetta di attuare misure che siano gradite sia all'azienda che ai dipendenti. Laddove ciò non sia possibile, la vostra azienda dovrà prendere in considerazione la possibilità di offrire metodi di accesso alternativi o di fornire dispositivi aziendali ai dipendenti.

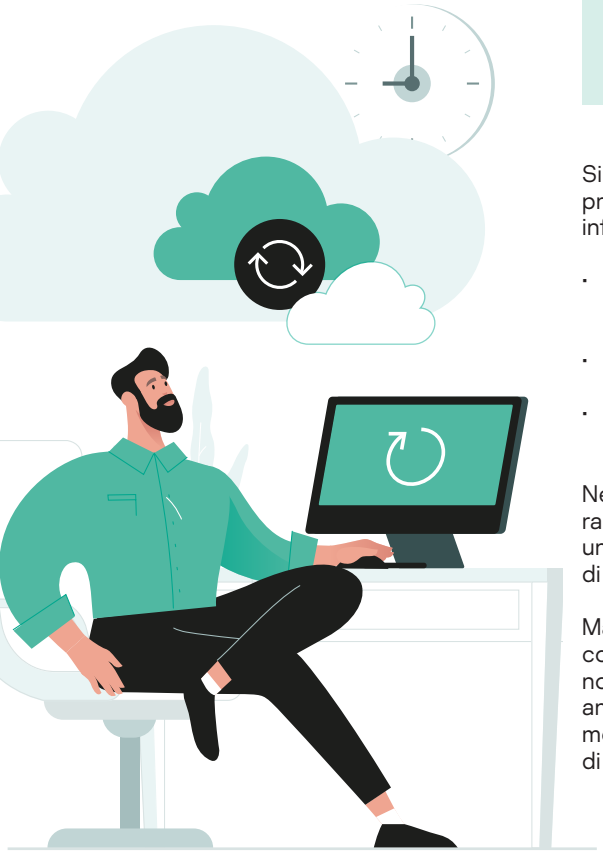
3. Configurazioni di backup

Una volta che i file sono stati criptati, le opzioni sono due: pagare il riscatto o recuperare copie "pulite" dei file dal backup, e questo implica una routine di backup robusta e affidabile anche per i dispositivi endpoint.

In una situazione ideale, i dipendenti non avrebbero la possibilità di archiviare i dati aziendali in locale ma, nel contesto attuale, è probabile che salvino i documenti nell'unità locale, spesso nella cartella Download o sul Desktop.

Per una maggiore sicurezza durante lo smart working, vanno tenuti in considerazione i seguenti fattori:

- **Con quale probabilità i dati aziendali possono essere archiviati in locale?**
- **Quali dati vengono salvati?**
- **Quali sono i rischi se questi file vengono criptati o resi inaccessibili?**
- **Come possiamo eseguire il backup di questi dati?**



Si tratta di una sfida significativa all'esterno del perimetro di rete. La risoluzione del problema dipenderà dall'architettura tecnica e, in una certa misura, dalle capacità informatiche dell'utente finale. Tra le opzioni da tenere in considerazione sono incluse:

- Sincronizzazione dei dati nelle cartelle selezionate in archivi cloud o altri servizi remoti, preferibilmente con backup immutabili che non possano essere sovrascritti o modificati.
- Esecuzione del backup in un'unità rimovibile locale.
- Fare affidamento su funzionalità integrate nel sistema operativo per creare copie shadow automatiche e punti di rollback.

Nessuna di queste potenziali soluzioni è ideale perché esiste la minaccia intrinseca che ransomware e file criptati vengano replicati nel backup. Tuttavia, è necessario identificare un modo per acquisire i dati archiviati in locale, se non altro per soddisfare gli obblighi di conformità e protezione dei dati.

Ma va sempre tenuto a mente che il backup dei dati è l'ultima linea di difesa a cui ricorrere contro i file criptati dal ransowmare, senza tralasciare il fatto che il backup e il ripristino non proteggeranno la vostra azienda dalle fughe di dati o dal doxxing. I criminali possono anche chiedere un ulteriore riscatto minacciando di esporre informazioni sensibili. L'unico modo per difendersi da questi attacchi ai danni della **riservatezza** è impedire ai criminali di accedere agli endpoint.

4. Alleggerire le operazioni

Più sono i dati e le applicazioni contenuti in un dispositivo endpoint, più aumentano le potenziali vulnerabilità da sfruttare e l'appetibilità del computer in questione per gli hacker Pertanto, **riducendo** la quantità di applicazioni e dati archiviati in locale, si ridurrà l'impatto di un'infezione ransomware.

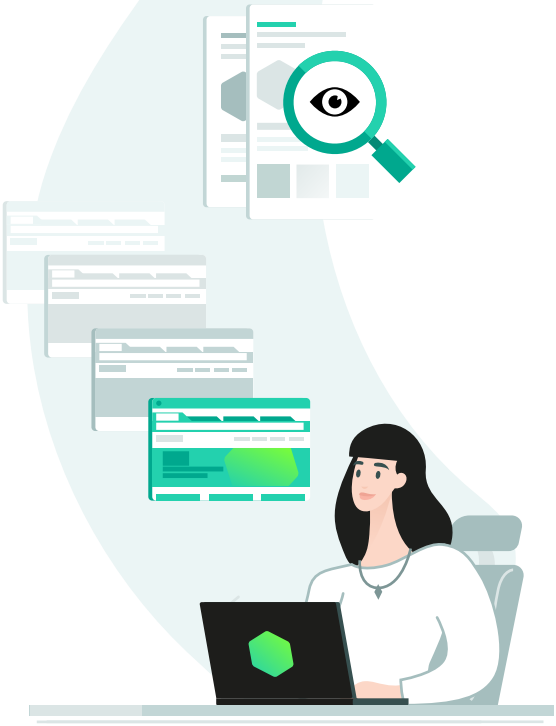
I servizi cloud consentono di ridurre il sovraccarico delle applicazioni, riducendo al minimo la quantità di dati archiviati nel dispositivo locale. Gli strumenti di posta elettronica e produttività ora possono essere eseguiti come app Web nel cloud, ad esempio garantendo un trasferimento di dati pressocché nullo. Molti, in particolare i servizi di posta elettronica, offriranno anche una protezione avanzata dal malware per esaminare, rilevare e bloccare gli allegati sospetti prima che gli utenti possano scaricarli.

La virtualizzazione offre un'altra possibilità. Utilizzando streaming desktop e applicazioni, gli utenti possono connettersi a una sessione ospitata nel data center o nel cloud aziendale. La sessione ospitata offre una sessione simile a un desktop per l'utente finale ma, ancora una volta, tutti i dati e le attività di elaborazione vengono completati all'interno del sistema virtualizzato.

Le sessioni desktop remoto (RDP) sono considerate il principale vettore di attacco singolo per il ransomware[8]. Ma se configurate correttamente, creano un'utile sandbox tra il dispositivo endpoint e i sistemi aziendali, come dimostra l'ampio uso delle sessioni RDP all'interno della rete aziendale.

È possibile ottenere gli stessi vantaggi per i lavoratori da remoto rafforzando la sicurezza degli endpoint, ovvero:

- **Utilizzando criteri per password complesse per prevenire gli attacchi di forza bruta.**
- **Implementando l'autenticazione a più fattori per impedire il dirottamento delle sessioni.**
- **Utilizzando connessioni VPN per tutto il traffico tra endpoint e server RDP.**
- **Valutando e rafforzando le regole del firewall del perimetro di rete per prevenire le connessioni non autorizzate.**
- **Utilizzando strumenti di protezione EDR per valutare le attività al fine di identificare e bloccare automaticamente le attività sospette.**
- **Scegliendo porte di connessione RDP non standard per evitare i tentativi di hacking speculativi.**



In definitiva, la chiave è impedire che hacker e malware compromettano la sessione e la connessione RDP, per proteggere adeguatamente l'endpoint dell'utente.

5. Formazione per l'utente finale

I dipendenti sono la risorsa più preziosa di qualsiasi azienda e, se in grado di muoversi adeguatamente, possono svolgere un ruolo importante nella prevenzione della diffusione del ransomware. Tutti i dipendenti, non solo quelli che lavorano da remoto, dovrebbero ricevere una formazione regolare in modo da essere dotati di ogni strumento necessario a identificare potenziali attacchi alla sicurezza informatica ed essere pronti a prendere i giusti provvedimenti. Ogni giorno, il 2% dei dipendenti fa clic su un collegamento di phishing[9] e tassi simili sono prevedibili anche per il ransomware.

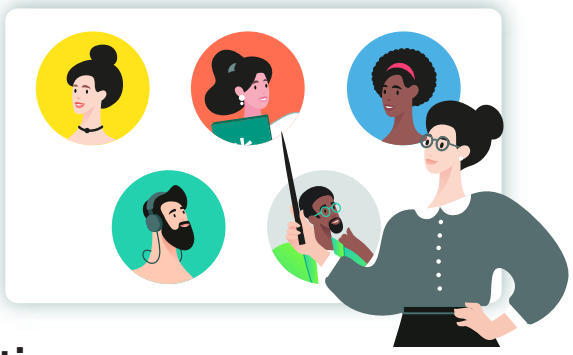
La formazione deve essere interattiva, pratica e a cadenza regolare: dopotutto, le minacce alla sicurezza informatica sono in continua evoluzione. Un'unica presentazione sull'identificazione dei messaggi e-mail di phishing e dei file eseguibili sospetti diventerà presto obsoleta e cadrà nel dimenticatoio. Ecco alcuni fattori da considerare quando si definisce la formazione sulla sicurezza informatica per chi lavora da remoto.

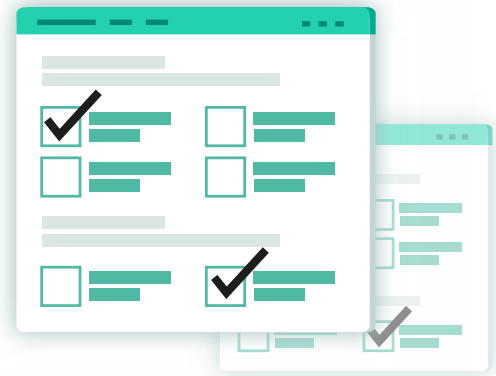
[8]How to secure RDP from ransomware attackers – Emsisoft –https://blog.emsisoft.com/en/36601/how-to-secure-rdp-from-ransomware-attackers/

[9]Mobile Security Index 2020 Report – Verizon – https://www.verizon.com/business/en-gb/resources/reports/mobile-security-index/2020/mobile-threat-landscape/user-threats/

Personalizzate la formazione

Gli attacchi ransomware più efficaci sono mirati con attenzione a persone e ruoli specifici. Di conseguenza, è opportuno personalizzare la formazione. Finanza, marketing, risorse umane e dirigenti dovranno affrontare attacchi leggermente diversi, quindi istruirli in modo a loro familiare sulle potenziali minacce che affronteranno sarà un vantaggio sia per loro che per l'azienda.



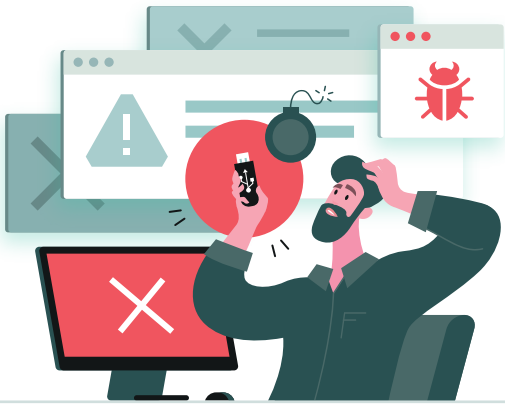


Testate i dipendenti

La teoria ha poco valore se non è accompagnata dalla pratica, specialmente quando la posta in gioco è così alta. Test di routine e regolari assicurano che i dipendenti siano sempre in grado di mettere in pratica la loro formazione quando necessario. Le valutazioni di routine metteranno in evidenza anche le lacune o le opportunità di miglioramento e la strategia di sicurezza della vostra azienda.

Andate oltre il phishing

Gli allegati pericolosi e di phishing sono la fonte più ovvia di infezione ransomware. Tuttavia, ci sono altri fattori di cui gli utenti finali devono essere a conoscenza. Le unità rimovibili infette, i siti Web dannosi e la contaminazione tra lavoro e attività personali possono introdurre malware nell'endpoint e nella più ampia rete aziendale. È necessario assicurarsi che i dipendenti siano formati adeguatamente anche per rilevare questi potenziali problemi.



Mantenete vivo l'interesse e il divertimento

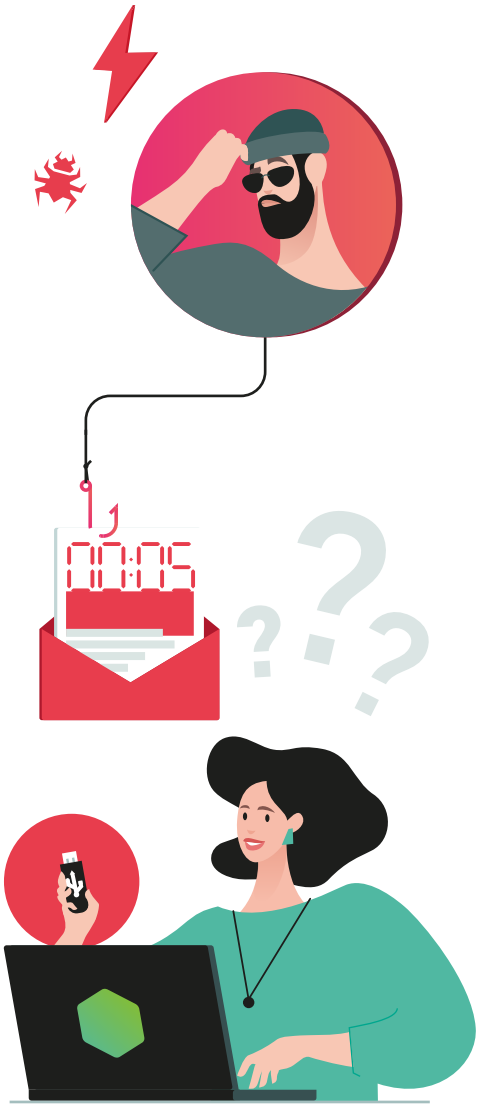
La sicurezza informatica può essere noiosa, in particolare se non è una delle vostra responsabilità di base: è infatti molto improbabile che i vostri utenti finali leggano (o capiscano) i briefing settimanali del National Cyber Awareness System degli Stati Uniti. L'uso delle attività di gamification incentiverà l'interesse e l'engagement, in particolare quando i concetti diventano più complessi. Stabilire obiettivi e sfide, incentivare lo spirito competitivo e rendere il processo divertente incoraggerà i dipendenti a rimanere in contatto e a migliorare costantemente le proprie conoscenze e abilità.

Investire negli utenti finali è un passo importante per rafforzare la difesa degli endpoint. In effetti, ridurre al minimo l'errore umano è forse la forma più efficace di prevenzione dal ransomware. Aiuterà inoltre i dipendenti a svolgere un ruolo efficace nelle primissime fasi di un'infezione ransomware, contribuendo a ridurre al minimo la diffusione e l'impatto complessivo sull'azienda.

6. Pianificazione della risposta agli incidenti

Ben il 32% delle aziende non dispone di un piano formale di risposta per affrontare incidenti di sicurezza informatica come un'epidemia di ransomware[10]. Queste organizzazioni stanno assumendo un livello di rischio ingiustificato in quanto tutte, prima o poi, dovranno affrontare un incidente malware.

La creazione di un piano di risposta agli incidenti aiuterà la vostra azienda a valutare le vulnerabilità e ad adottare le misure appropriate per mitigarle. Il piano aiuterà anche ad accelerare la risposta, fondamentale quando si ha a che fare con una tipologia di ransomware in cui ogni secondo può fare la differenza.



Ogni piano di ripristino di emergenza degli endpoint, seppur diverso da organizzazione a organizzazione, deve includere:

- **Una strategia di comunicazione.** Dovete assicurarvi che le giuste informazioni raggiungano le parti interessate al momento opportuno e che i vostri dipendenti in smart working siano in grado di mettersi in contatto con esperti che possano aiutarli nelle prime fasi di un'infezione.
- **Un piano di attacco.** Stabilite come determinare la gravità di un attacco e la modalità di risposta. Pagherete il riscatto o proverete a recuperare i dati dal backup?
- **Documentazione accessibile.** È molto probabile che un'infezione degli endpoint impedisca ai dipendenti di accedere ai playbook o alle istruzioni per rispondere al ransomware. Dovete assicurarvi che ci sia sempre un modo per accedere a queste informazioni, anche in caso di inattività dei sistemi.
- **Guida per i dipendenti.** Non appena viene rilevato un problema, è necessario assegnare uno specialista in grado di assistere il dipendente in remoto. Lo specialista potrà illustrare le procedure iniziali di mitigazione e ripristino, nonché raccogliere informazioni da includere nel rapporto da inoltrare alle autorità di regolamentazione, se necessario.
- **Vigilanza ottimizzata.** Non appena viene rilevata un'infezione ransomware in un endpoint remoto, il team di sicurezza IT deve aumentare i livelli di monitoraggio e reporting per valutare se anche i sistemi centrali sono stati compromessi. I tecnici possono attivare il piano di ripristino di emergenza, se richiesto.

Un piano di ripristino di emergenza ben strutturato consente all'azienda di ridurre l'impatto del malware, contenendone la diffusione molto prima che raggiunga sistemi e dati importanti.

[10]Cyber Security Breaches Survey 2021 – UK Department for Digital, Culture, Media & Sport – https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/cyber-security-breaches-survey-2021

Conclusione

Da molti anni una delle principali preoccupazioni dei dirigenti IT riguarda giustamente lo smart working. Tuttavia, gli eventi recenti hanno cambiato per sempre il modo di lavorare e lo smart working è ormai un aspetto fondamentale in ogni azienda.

Allo stesso tempo, il ransomware è diventato uno strumento standard nel kit dei cybercriminali. Gli attacchi ai danni delle organizzazioni sono frequenti, efficaci e potenzialmente devastanti. Lo smart working ha ampliato le superfici di attacco, pertanto è estremamente probabile che ogni azienda risenta delle conseguenze.

Proteggere gli endpoint dal ransomware dovrebbe quindi essere una priorità strategica. In caso contrario, il rischio è che per l'azienda sia già troppo tardi per rispondere in modo efficace quando si verifica l'inevitabile.

I sei fattori delineati in questo whitepaper aiuteranno immediatamente la vostra azienda a essere più pronta a un eventuale attacco ransomware. Comprendere questi fattori migliorerà immediatamente la strategia di sicurezza degli endpoint:

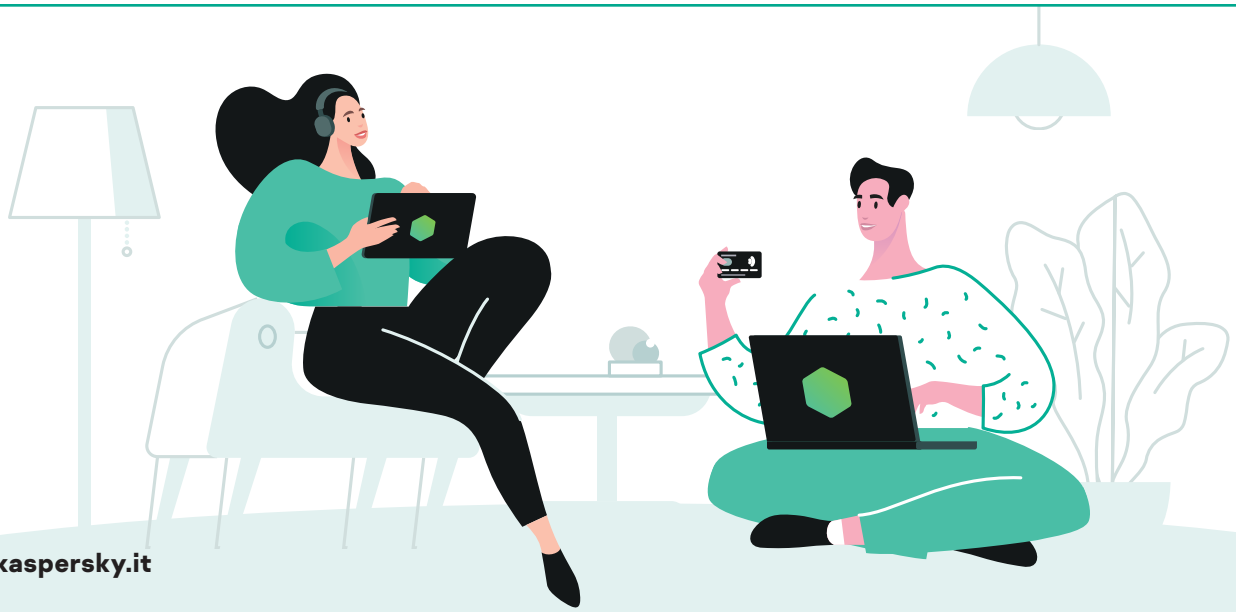
1. Rilevamento e rimozione del malware
2. Configurazione dei dispositivi
3. Backup e ripristino dei dati
4. Alleggerire le operazioni
5. Formazione
6. Pianificazione del ripristino di emergenza

Se volete sapere di più sulla protezione dei lavoratori in smart working e del resto dell'organizzazione dal ransomware, Kaspersky può aiutarvi. La soluzione Kaspersky Optimum Security cloud-native vi consente di eseguire l'upgrade della protezione contro minacce nuove, sconosciute ed elusive, attraverso un rilevamento e una risposta efficaci alle minacce e un monitoraggio della sicurezza 24 ore su 24, 7 giorni su 7, senza complessità o costi proibitivi. Più visibilità. Più capacità. Più controllo.

Ulteriori informazioni sono disponibili sul sito Web: go.kaspersky.com/it_optimum

Letture consigliate:

La storia dell'anno: il ransomware nei titoli dei giornali
Scopri qual è il livello di protezione endpoint più adatto a te
Guida all'acquisto EDR
Aumenta la sicurezza informatica per i team di lavoro in remoto, rafforzando il sistema



www.kaspersky.it

kaspersky BRING ON THE FUTURE