semperis

SUPPLEMENTO RIGUARDANTE L'ITALIA

2024

Ransomware Holiday Risk Report

- Indicazioni di esperti per rafforzare la difesa contro il ransomware, particolarmente durante periodi ad alto rischio come i giorni di ferie, i fine settimana e le transizioni aziendali
- Dati approfonditi sugli schemi di attacco ransomware rivelano che molte aziende mancano di difese adeguate contro attacchi sferrati durante periodi di distrazione
- Nuove prove che le aziende normalmente sopravvalutano le loro capacità di difesa contro attacchi basati sull'identità

"Durante i giorni di ferie e i fine settimana le aziende non dovrebbero diminuire la vigilanza contro gli attacchi informatici. Anzi, dovrebbero considerare l'opportunità di rafforzare le difese contro attacchi ransomware. La migliore garanzia contro le minacce durante questi periodi è rappresentata dalla consapevolezza e da un affidabile piano di backup e ripristino pronto per essere implementato quando sono in corso minacce".

Bruno Filippelli
Direttore Semperis

Panoramica sul **rischio di ransomware**

Gli attacchi ransomware non rispettano gli orari di lavoro e spesso gli attacchi vengono sferrati con velocità superiore alla sola capacità di intervento delle persone, così che per mitigare il rischio sono necessarie strategie automatizzate di gestione delle identità.

Gli hacker colpiscono durante periodi di assenza o distrazione, come i giorni di ferie, i fine settimana e gli eventi aziendali, comprese fusioni e acquisizioni.

In tutto il mondo le aziende sono impegnate in una battaglia contro gli attacchi informatici e particolarmente di ransomware. All'aumentare della posta in gioco è sempre più evidente che Microsoft Active Directory è uno degli obiettivi principali degli hacker e che la rilevazione delle minacce per le identità e la risposta (ITDR) è un aspetto chiave sia della resilienza informatica sia di quella operativa.

Per esaminare tendenze nella frequenza, gravità e impatto del ransomware, Semperis ha stretto una partnership con la società di ricerca internazionale Censuswide per condurre uno studio completo su diversi settori in vari paesi – Stati Uniti, Regno Unito, Francia e Germania. Il primo rapporto sui risultati – *2024 Ransomware Risk Report* – ha rivelato che gli attacchi ransomware sono incessanti e costosi, mentre un secondo rapporto – *2024 Ransomware Holiday Risk Report* – ha esaminato la tempistica degli attacchi sferrati durante periodi di distrazione aziendale (giorni feriali, fine settimana ed eventi importanti quali fusioni, IPO e sospensioni dal lavoro) e potenziali lacune nelle difese di cybersecurity delle aziende.

Questo supplemento espande la nostra ricerca. Abbiamo chiesto a 100 aziende italiane di rispondere a un sottoinsieme di domande del nostro sondaggio per determinare la loro esperienza in merito agli argomenti discussi nei rapporti precedenti.

ESPERTI CHE HANNO COLLABORATO

Mickey Bresman
Amministratore delegato Semperis

Sean Deuby
Tecnologo capo Semperis (Nord America)

Bruno Filippelli
Direttore Semperis

Guido Grillenmeier
Tecnologo capo Semperis (EMEA)

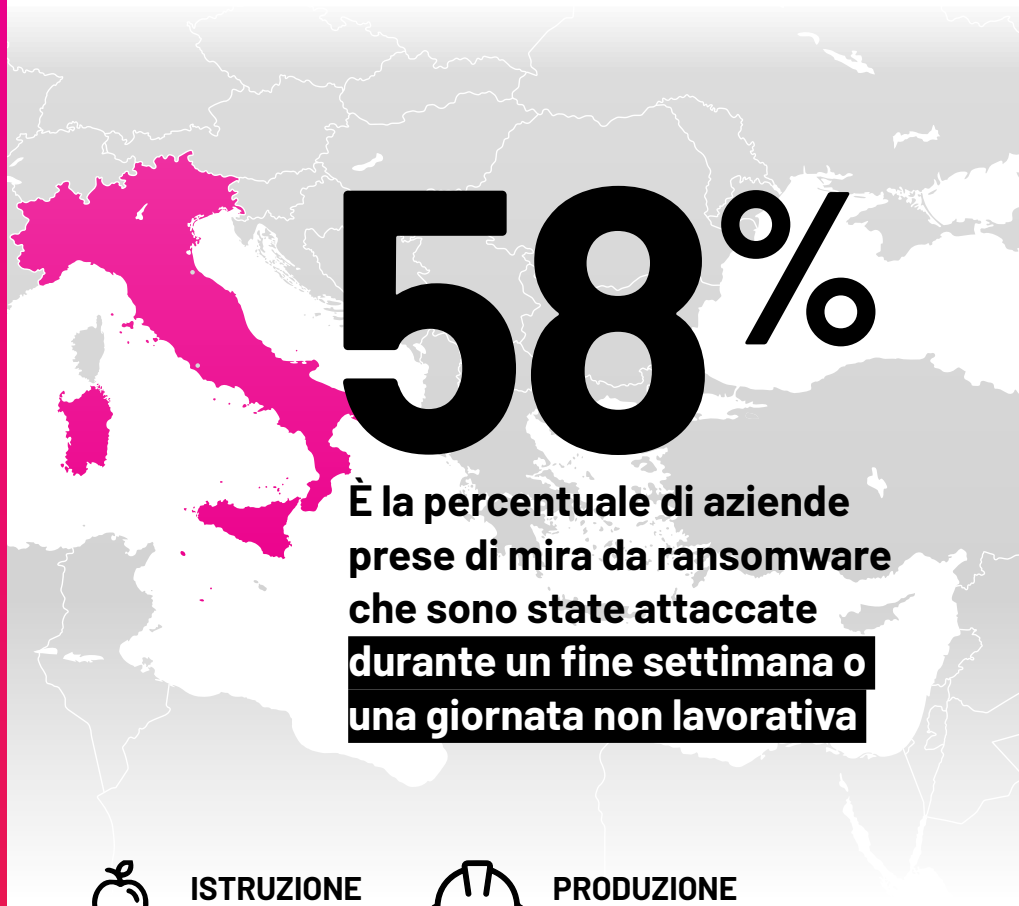
Simon Hodgkinson
Consulente strategico Semperis, ex Direttore sicurezza informatica presso BP

Chris Inglis
Consulente strategico Semperis, ex Direttore cybersecurity degli Stati Uniti

Gli hacker non vanno in vacanza

"Quando un hacker si introduce nei sistemi di un'azienda, specialmente durante una giornata non lavorativa o un fine settimana, quando il personale è ridotto, è possibile che nessuno se ne accorga subito. Durante tali periodi le aziende sono meno attente e più vulnerabili, e gli hacker lo sanno".

Guido Grillenmeier
Tecnologo capo (EMEA) presso Semperis



58%

È la percentuale di aziende prese di mira da ransomware che sono state attaccate durante un fine settimana o una giornata non lavorativa

ISTRUZIONE
79%

PRODUZIONE
75%

ATTIVITÀ FINANZIARIE
78%

IT/TELECOMUNICAZIONI
68%

ASSISTENZA SANITARIA
74%

VIAGGI/TRASPORTO
75%

Gli hacker colpiscono quando il personale del centro sicurezza (SOC) è ridotto

Il SOC della tua azienda è operativo 24/7/365?

94%

SÌ

"La cybersecurity non può aumentare e diminuire. Deve essere costante e sempre presente".

Chris Inglis
Consulente strategico Semperis, ex Direttore cybersecurity degli Stati Uniti

	TUTTI	ISTRUZIONE	ATTIVITÀ FINANZIARIE	ASSISTENZA SANITARIA	PRODUZIONE	IT/ TELECOMUNICAZIONI	VIAGGI/ TRASPORTO
Sì (totale)*	**94%**	**100%**	**100%**	**100%**	**86%**	**93%**	**100%**
Sì *(in outsourcing/ ibrido)*	**23%**	0%	8%	0%	29%	26%	0%
Sì *(interno)*	**71%**	100%	92%	100%	57%	67%	100%

Durante i fine settimana e le giornate non lavorative riduci il personale del SOC e se sì, in che misura?

82% È la percentuale di aziende intervistate che **hanno ridotto** il personale **anche del 50%**

Aziende nel settore viaggi/trasporto che indicavano di essere più disposte a **mantenere il personale** al

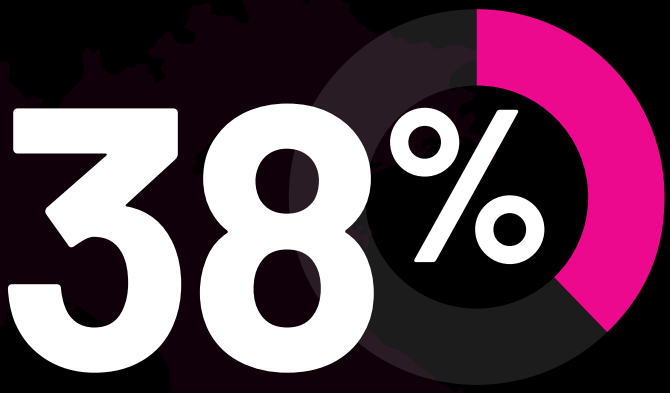
50% **O PIÙ** durante i fine settimana e le giornate non lavorative.

59% È la percentuale di aziende che **hanno ridotto** il personale del SOC durante i fine settimana e le giornate non lavorative per **proteggere l'equilibrio lavoro/vita privata**

Gli attacchi vengono sferrati durante periodi di distrazione aziendale

"Non sono per niente sorpreso dalla percentuale di aziende che vengono attaccate dopo un evento aziendale. ... Durante eventi importanti, la priorità per l'azienda è completare l'evento – non è la sicurezza".

Simon Hodgkinson
Consulente strategico Semperis, ex Direttore sicurezza informatica presso BP



È la percentuale di aziende **prese di mira** da un attacco ransomware **dopo un evento aziendale importante**

ISTRUZIONE
50%

ATTIVITÀ FINANZIARIE
33%

IT/TELECOMUNICAZIONI
42%

La protezione delle identità è essenziale per la resilienza del business

"Molte aziende concentrano le risorse sulla protezione degli endpoint ma gli hacker spesso li bypassano completamente. Una volta introdottisi, prendono di mira il sistema di gestione delle identità – l'asse portante del network. Cosa accade quando lo violano? Grazie al controllo sul sistema di gestione delle identità, hanno accesso all'intera infrastruttura. Senza un sistema di gestione delle identità resiliente, le altre difese crollano".

Bruno Filippelli
Direttore Semperis

89%

È LA PERCENTUALE DI AZIENDE CHE HANNO SPECIFICATO UN BUDGET PER LA DIFESA DI SISTEMI DI GESTIONE DELLE IDENTITÀ ESSENZIALI COME ACTIVE DIRECTORY

Quanto tempo è trascorso prima che le aziende ripristinassero una funzionalità IT minima?

- **21%** MENO DI 5 ORE
- **31%** 1-7 ORE
- **44%** 5 ORE - 1 GIORNO
- **4%** OLTRE 7 GIORNI

87%

È la percentuale di aziende intervistate che affermano di avere un **piano adeguato di ripristino delle identità**

- **ISTRUZIONE** 50%
- **ATTIVITÀ FINANZIARIE** 92%
- **ASSISTENZA SANITARIA** 100%
- **PRODUZIONE** 71%
- **IT/ TELECOMUNICAZIONI** 89%
- **VIAGGI/TRASPORTO** 50%

Bilanciare le priorità aziendali

Si può essere, e si viene, colpiti da attacchi ransomware in modo del tutto imprevisto. Nessuna impresa – indipendentemente dal paese, dal settore o dallo stato del SOC – dovrebbe sottovalutare la necessità di una vigilanza costante. Inoltre attività efficaci di difesa contro il ransomware devono includere un piano per la difesa e il ripristino di Active Directory. Quindi, i responsabili aziendali, tecnologici e della sicurezza quali misure possono prendere per ridurre la probabilità che un attacco ransomware riesca e migliorare la loro capacità di opporsi recisamente agli hacker? I nostri esperti suggeriscono tre misure in iniziali.

1

I più alti dirigenti devono definire come **priorità aziendali** sia la **difesa contro il ransomware** sia la **sicurezza delle identità.**

2

Soluzioni ITDR affidabili e **partner esperti** possono aiutare i responsabili della sicurezza a **controbilanciare i problemi di riduzione del personale.**

3

La sicurezza di Active Directory dovrebbe essere un **aspetto fondamentale** di qualsiasi fusione o acquisizione.

"Negli ultimi anni è aumentata in modo significativo la consapevolezza del ruolo cruciale svolto dalle identità in relazione alla sicurezza. Sebbene la ITDR sta finalmente ricevendo l'attenzione che merita, c'è ancora molto da fare ai fini della protezione e sicurezza dei sistemi di gestione delle identità".

Mickey Bresman
Amministratore delegato Semperis

METODOLOGIA

Per condurre questo studio abbiamo stretto una partnership con vari esperti presso Censuswide, una società di ricerche di mercato internazionali con sede a Londra. Censuswide ha intervistato 100 professionisti IT e della sicurezza in Italia in vari settori – istruzione, attività finanziarie, assistenza sanitaria, produzione e utility, IT e telecomunicazioni, viaggi e trasporto.

COME MENZIONARE LE INFORMAZIONI DI QUESTO RAPPORTO

I dati contenuti in questo rapporto vengono presentati come fonte di informazioni per la comunità di esperti nella cybersecurity e delle aziende che a questi si rivolgono. Semperis incoraggia il lettore a condividere i nostri risultati. Per menzionare statistiche, fare riferimento al documento *Semperis 2024 Ransomware Holiday Report*: *Supplemento riguardante l'Italia* e indicare il link al rapporto, scaricabile da https://www.semperis.com/resources/italia-ransomware-risk. Per intervistare esperti Semperis, contattare Bill Keeler a billk@semperis.com. Infine, saremo lieti di ricevere domande o riflessioni sull'argomento del ransomware e della resilienza. Trova Semperis su LinkedIn.

PROFILO DI SEMPERIS

Per i team responsabili della sicurezza di ambienti ibridi e multicloud, Semperis garantisce l'integrità e la disponibilità di servizi cruciali delle directory aziendali in ogni fase della cyber kill chain e riduce fino al 90% il tempo di ripristino. Sviluppata appositamente per difendere contro le intrusioni gli ambienti delle identità ibridi – Active Directory, Entra ID e Okta – la tecnologia brevettata Semperis protegge oltre 100 milioni di identità contro attacchi informativi, violazioni dei dati ed errori operativi. Le principali aziende mondiali contano su Semperis per individuare vulnerabilità delle directory, intercettare attacchi informatici in corso e ripristinare rapidamente i dati dopo attacchi ransomware e altre emergenze riguardanti la loro integrità. Semperis ha sede a Hoboken, nel New Jersey, e opera a livello internazionale – il suo team di ricerca e sviluppo è distribuito tra gli Stati Uniti, il Canada e Israele.

Semperis ospita la premiata serie di podcast e convegni Hybrid Identity Protection e ha creato gli strumenti di difesa della cybersecurity Active Directory ibridi per la community del settore, Purple Knight e Forest Druid. Semperis ha ricevuto i riconoscimenti più prestigiosi del settore – recentemente è stata inserita nell'elenco Inc. Magazine dei migliori luoghi di lavoro nel 2024 ed è risultata prima tra le imprese di cybersecurity a più rapida crescita negli Stati Uniti nella classifica compilata dal Financial Times. Semperis è un co-selling partner della Microsoft Enterprise Cloud Alliance e un membro della Microsoft Intelligent Security Association (MISA).

Per saperne di più: https://www.semperis.com

semperis

+1-703-918-4884 | info@semperis.com | www.semperis.com

5 Marine View Plaza, Suite 102, Hoboken, NJ 07030 USA