Report globale di Netwrix sui rischi IT del 2018: riepilogo generale

Questo report si basa sulle risposte di 1.558 società di varie dimensioni, zone e settori. Riassume le esperienze e i programmi che queste società mettono in atto per affrontare sei tipologie di rischi IT: danni fisici, furto di proprietà intellettuale (IP), perdita o violazione dei dati, interruzione del sistema e sanzioni di conformità.

Il report indica i seguenti risultati chiave:

- La maggior parte delle aziende ritiene che gli attacchi degli hacker siano la minaccia più pericolosa, ma in realtà sono i propri dipendenti che causano la maggior parte degli incidenti di sicurezza, per mezzo di azioni volontarie o accidentali.
- Non tutti i controlli di sicurezza critici vengono revisionati regolarmente, come richiesto dalle best practice. I controlli più trascurati includono l'eliminazione di dati obsoleti e non necessari e la classificazione dei dati. Questi controlli sono effettuati raramente o per nulla rispettivamente dal 20% e dal 14% delle società.
- Sebbene il 70% delle aziende abbia condotto una valutazione del rischio IT almeno una volta, solo il 33% rivaluta regolarmente i propri rischi IT.
- Il 44% degli intervistati non sa, o non è sicuro, del modo in cui i propri dipendenti utilizzino i dati sensibili.
- Nonostante ciò, oltre il 60% degli intervistati ritiene che il livello di visibilità della propria rete sia sufficiente, rivelando un falso senso di sicurezza.
- Solo il 17% delle società possiede un piano di intervento in caso di incidente; il 42% possiede solo una bozza o non possiede alcun piano.

Località

America del Nord	43%
Europa	29%
Asia/Pacifico	19%
Sud America	6%
Africa	1%
Medio Oriente	2%

Numero di dipendenti

1–9	4%
10–99	19%
100–499	28%
500–999	13%
1,000–4,999	14%
5,000–9,999	12%

10,000 o più	10%

Dati approfonditi sugli intervistati italiani

Numero di intervistati: 164

Sono rappresentati da:

• Aziende di medie dimensioni con 100-499 dipendenti (31%)
• Piccole aziende con 10-99 dipendenti (28%)
• Grandi aziende con 500-999 dipendenti (9%)

Complessivamente il 69% delle società ha effettuato una valutazione del rischio IT almeno una volta. Solo il 14% delle aziende intervistate rivaluta i propri rischi IT almeno una volta al trimestre. Complessivamente, il 36% esegue questo una volta all'anno; Il 18% delle aziende non possiede un programma specifico per la valutazione del rischio IT.

Agli intervistati è stato chiesto di rispondere ad alcune domande a scelta multipla. Le risposte scelte più di frequente sono presentate nei risultati.

Risultati complessivi delle risposte alla domanda "Quali sono i settori in cui la tua azienda deve migliorare (secondo il framework NIST)?" per ciascuno dei sei rischi:

- Identificazione 53%
- Protezione 56
- Individuazione 59%
- Risposta 41%
- Recupero 24%

Quali di questi rischi IT sono i più critici per la tua azienda?

- Violazione dei dati 58%
- Perdita di dati 59%
- Interruzione del sistema 32%

Quale di questi aggressori potrebbe provocare più danni?

- Dipendenti infedeli o scontenti 71%
- Utenti aziendali abituali 39%

- Cyber-terroristi 28%

Quale tipologia di utenti è potenzialmente più dannosa?

- Membri del team IT 55%
- Dipendenti regolari 53%
- Consulenti 28%
- Manager di medio livello 21%
- Manager di livello C 11%

Rischio 1. Danno fisico.

Quali problemi legati al danno fisico costituiscono il rischio principale per la tua società?

- Errori umani 74%
- Interruzioni di corrente 61%
- Guasti hardware 56%

Quali aggressori rappresentano il rischio più grande per le risorse fisiche della tua società?

- Hacker 52%
- Dipendenti dimissionari e licenziati 50%
- Utenti aziendali abituali 45%

Quali problematiche legate ai danni fisici hai riscontrato nell'ultimo anno?

- Errori umani 59%
- Guasti hardware 50%
- Interruzioni di corrente 32%

In genere chi è responsabile dei problemi legati al danno fisico?

- Membri del team IT 45%
- Utenti aziendali abituali 32%

Quali aree della sicurezza informatica devono essere migliorati nella tua azienda per evitare danni fisici?

- Individuazione 62%
- Risposta 57%

Rischio 2. Furto IP

Quali problemi legati al furto della proprietà intellettuale (IP) costituiscono il rischio più grande per la tua società?

- Errori umani 72%
- Infiltrazioni di malware 65%
- Spyware 50%

Quali aggressori rappresentano il rischio più grande per la tua azienda in termini di furto della IP?

- Dipendenti dimissionari e licenziati 37%
- Hacker 44%
- Utenti aziendali abituali 39%

Quali problemi legati al furto della IP hai riscontrato nell'ultimo anno?

- Non abbiamo avuto incidenti relativi al furto della IP 37%
- Errori umani 32%
- Infiltrazioni di malware 26%

Di solito chi è coinvolto in problemi legati al furto di proprietà intellettuale e allo spionaggio informatico?

- Membri del team IT 42%
- Utenti aziendali abituali 45%
- Dipendenti dimissionari e licenziati 36%

Quali sono le aree della sicurezza informatica che devono essere potenziate dalla tua azienda per evitare il furto della IP?

- Individuazione 58%
- Protezione 53%

Rischio 3. Perdita di dati

Quali problemi legati alla perdita di dati costituiscono il rischio più grande per la tua società?

- Errori umani 81%
- Infiltrazioni di malware 56%
- Eliminazioni intenzionali 19%

Quali aggressori rappresentano il rischio più grande per la tua società in termini di perdita di dati?

- Dipendenti dimissionari e licenziati 37%

- Hacker 35%
- Utenti aziendali abituali 31%

Quali problemi legati alla perdita di dati hai riscontrato nell'ultimo anno?

- Errori umani 44%
- Guasti hardware 31%
- Infiltrazioni di malware 19%

Di solito chi è coinvolto in problemi legati alla perdita di dati?

- Utenti aziendali abituali 50%
- Membri del team IT 38%
- Dipendenti dimissionari e licenziati 25%

Quali sono le aree della sicurezza informatica che devono essere potenziate nella tua azienda per evitare la perdita di dati?

- Protezione 62%
- Individuazione 66%
- Identificazione 44%

Rischio 4. Violazione dei dati

Quali problemi legati alla violazione dei dati costituiscono il rischio più grande per la tua società?

- Condivisione di password 75%
- Errori umani 71%
- Attacchi di phishing 64%

Quali aggressori rappresentano il rischio più grande per la tua società in termini di violazione dei dati?

- Hacker 43%
- Membri del team IT 54%
- Dipendenti dimissionari e licenziati 23%

Quali problemi legati alla violazione dei dati hai riscontrato nell'ultimo anno?

- Errori umani 36%
- Non abbiamo avuto incidenti relativi alla violazione dei dati 40%
- Condivisione password 28%

Di solito chi è coinvolto in problemi relativi alla violazione dei dati?

- Utenti aziendali abituali 46%
- Membri del team IT 38%
- Dipendenti dimissionari e licenziati 31%

Quali sono le aree della sicurezza informatica che devono essere potenziate nella tua azienda per evitare violazioni dei dati?

- Identificazione 60%
- Protezione 57%
- Individuazione 71%

Rischio 5. Interruzione del sistema

Quali problemi legati all'interruzione del sistema costituiscono il rischio più grande per la tua società?

- Ransomware 70%
- Blackout elettrico 57%
- Errori umani 43%

Quali aggressori rappresentano il rischio più grande per la tua società in termini di interruzione del sistema?

- Hacker 57%
- Dipendenti dimissionari e licenziati 28%
- Consulenti 27%

Quali problemi legati all'interruzione del sistema hai riscontrato nell'ultimo anno?

- Blackout elettrico 43%
- Non abbiamo avuto incidenti relativi all'interruzione del sistema 28%
- Errori umani 21%

Di solito chi è coinvolto in problemi relativi all'interruzione del sistema?

- Membri del team IT 61%
- Utenti aziendali regolari 38%
- Dipendenti dimissionarie licenziati 15%

Quali sono le aree della sicurezza informatica che devono essere potenziate nella tua azienda per evitare interruzioni del sistema?

- Protezione 64%
- Individuazione 64%
- Identificazione 50%

Rischio 6. Non conformità

Complessivamente il 100% degli intervistati è conforme al GDPR.

Saresti pronto a un controllo di conformità se gli auditor bussassero a sorpresa alla tua porta domani? - 55%

Quali sono le aree della sicurezza informatica che devono essere potenziate nella tua azienda per evitare multe per mancanza di conformità?

- Identificazione 57%
- Protezione 50%
- Risposta 42%

Sei riuscito a prepararti per essere conforme al GDPR prima della scadenza?

- Sì 64%
- No 36%

Quanto sono cresciuti gli investimenti in sicurezza negli ultimi 3 anni? - 96%

Quanto aumenteranno i tuoi investimenti in sicurezza nei prossimi 5 anni? - 113%

Principi di sicurezza

Con quale frequenza effettui una revisione di ciascuno di questi controlli di base sulle sicurezza?

- Aggiornamento password utente. Almeno una volta a trimestre - 57%; due volte all'anno - 21%; una volta all'anno - 14%; una volta ogni 2-3 anni - 7%.
- Aggiornamento software (update). Almeno una volta a trimestre - 43%; due volte all'anno - 14%; una volta all'anno - 36%; una volta ogni 2-3 anni - 7%.
- Aggiornamento password amministratore. Almeno una volta a trimestre - 14%; due volte all'anno - 50%; una volta all'anno - 14%; una volta ogni 2-3 anni - 7%; raramente o mai - 7%.
- Controllo della sicurezza fisica dell'hardware. Almeno una volta a trimestre - 21%; due volte all'anno - 21%; una volta all'anno - 43%; una volta ogni 2-3 anni - 7%.
- Controllo della sicurezza dei dispositivi endpoint. Almeno una volta a trimestre - 7%; due volte all'anno - 21%; una volta all'anno - 43%; una volta ogni 2-3 anni - 14%; raramente o mai - 7%.
- Effettuare l'inventario delle risorse. Almeno una volta a trimestre - 7%; due volte all'anno - 7%; una volta all'anno il 57%; una volta ogni 2-3 anni 14%; raramente o mai - 7%.

- Controllo di cartelle e condivisioni disponibili per tutti. Almeno una volta a trimestre - 7%; due volte all'anno - 14%; una volta all'anno - 43%; una volta ogni 2-3 anni - 14%; raramente o mai - 21%.
- Aggiornamento dei diritti di accesso secondo il principio del privilegio minimo. Almeno una volta a trimestre - 7%; due volte all'anno - 14%; una volta all'anno - 43%; una volta ogni 2-3 anni - 14%; raramente o mai - 7%.
- Eseguire una valutazione delle vulnerabilità. Almeno una volta a trimestre - 7%; due volte all'anno - 7%; una volta all'anno - 36%; una volta ogni 2-3 anni - 29%; raramente o mai - 7%.
- Sbarazzarsi di dati obsoleti e non necessari. Almeno una volta a trimestre - 0%; due volte all'anno - 14%; una volta all'anno - 36%; una volta ogni 2-3 anni - 7%; raramente o mai - 29%.
- Controllo di tutti i software usati dai dipendenti. Almeno una volta a trimestre - 7%; due volte all'anno - 0%; una volta all'anno - 50%; una volta ogni 2-3 anni - 0%; raramente o mai - 21%.
- Classificare i dati in base alla loro sensibilità. Almeno una volta a trimestre - 7%; due volte all'anno - 7%; una volta all'anno - 36%; una volta ogni 2-3 anni - 0%; raramente o mai - 29%.

Sei sicuro di sapere dove risiedono tutti i tuoi dati nella tua infrastruttura IT?

- Sì 57%
- No 36%
- Non so 7%

Sei sicuro di sapere in che modo i tuoi dipendenti gestiscono dati sensibili?

- Sì 50%
- No 28%
- Non so 22%

La tua azienda possiede un piano di risposta agli incidenti?

- Non abbiamo un piano di risposta agli incidenti 30%
- Abbiamo una bozza 28%
- Abbiamo un piano approvato su una condivisione di file 14%
- Non so 14%
- Abbiamo un piano e forniamo formazione per i dipendenti 8%
- Lo diamo in outsourcing 6%