

2021年ランサムウェアの影響に関するレポートから得られる6つのポイント

Keeperは、ランサムウェア攻撃を受けたことのある全米の従業員2,000人にインタビューを行いました。6つの主要なポイントを以下にまとめました。

従業員の約1/3が

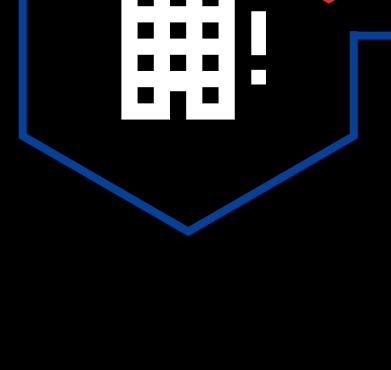
知らなかった

29% は、雇用主が攻撃を受ける前にランサムウェアが何であるかを知りませんでした



1

ランサムウェアが通常業務を大幅に妨害



2

77% が、攻撃後にシステムやネットワークにアクセスできなくなったと回答しました

64% が、攻撃後に組織が行った変更の結果、ログイン認証情報またはドキュメントを失ったと回答しました



3

ソーシャルエンジニアリングはランサムウェアにとって最大の武器

42% の攻撃はフィッシングメールが原因

21% は漏洩したパスワードが原因

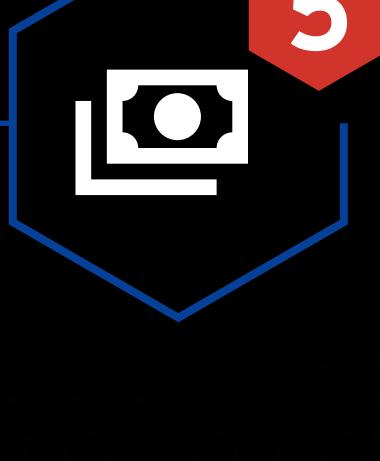


4

ランサムウェア攻撃被害後、多数の企業が最もセキュリティを強化

87% の被害を受けた企業が、後に厳格なセキュリティプロトコルを導入しました

62% が、多要素認証(MFA)を導入しました



5

身代金の支払いには別のコストがかかる

93% が、支払い後に他の分野で予算が削減されたと回答しました

49% が、雇用主が身代金を支払ったと答えました



6

ランサムウェアは強力な傷跡

64% が、ランサムウェア攻撃は企業の評判に悪影響を与えたと回答しました

[レポート全文をダウンロード](#)