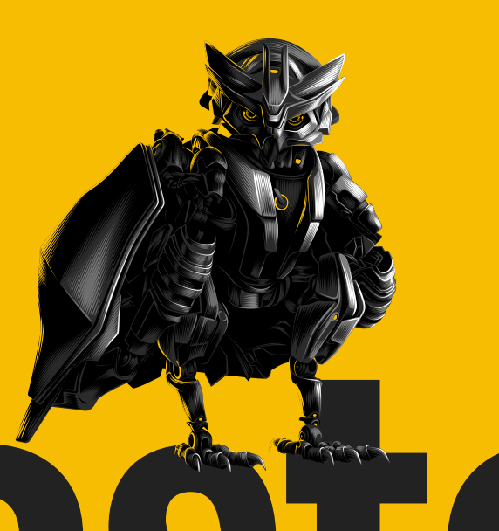
cybereason



Ransomware: die wahren Kosten

für deutsche Unternehmen 2024

Ergebnisse unserer jährlichen Umfrage zu den kommerziellen Auswirkungen von Ransomware in Deutschland

Im vergangenen Jahr haben Unternehmen in Deutschland – genauso wie Firmen in anderen nicht-englischsprachigen Ländern – mehr Angriffe und Sicherheitsverstöße gemeldet als je zuvor. **76 %** der untersuchten Unternehmen hatten eigenen Angaben zufolge ein Lösegeld gezahlt, doch nur bei der Hälfte von ihnen wurden die betroffenen Systeme einwandfrei wiederhergestellt. Zudem wurden die meisten wenige Monate später erneut angegriffen.

Angreifer gehen mit der Zeit

Angreifer nutzen generative KI zum Übersetzen und Skalieren von Angriffen in nicht-englischsprachigen Ländern. Oft nutzen sie zudem langsame, unauffällige Ansätze – in mehr als der Hälfte der Fälle mit einem Umweg über die Lieferkette – um sich Zugang zu Unternehmensinfrastrukturen zu verschaffen.

47% über einen Lieferkettenpartner

25% mit Beihilfe durch einen Insider

19% direkt

Worauf hatten sie es abgesehen?

- **Geistiges Eigentum/ Geschäftsgeheimnisse**
- **Anmeldedaten für Konten**
- **Personenbezogene Daten**
- **Kundendaten**
- **Informationen zum Gesundheitszustand von Personen**

Zahlen ist nicht die beste Lösung

Die meisten betroffenen Unternehmen zahlten das geforderte Lösegeld, aber **nur die Hälfte bekam ihre Systeme und Daten unbeschädigt zurück.** In den darauffolgenden sechs Monaten wurden allerdings **die meisten erneut angegriffen.**

76% **zahlten** das Lösegeld.

Aber **nur** **52%** von ihnen bekamen ihre Daten und Services unbeschädigt zurück.

76% wurden danach **erneut angegriffen.**

82% wurden **innerhalb von nur sechs Monaten erneut angegriffen.**

64% von ihnen sollten beim zweiten Angriff zudem **ein höheres Lösegeld** zahlen.

22% an denselben Erpresser

55% an einen anderen Erpresser

Lösegeldforderungen sind hoch

Lösegeldforderungen sind hoch, und sie **sind nur die Spitze des Eisbergs,** wenn man die wahren Kosten eines Cyber-Angriffs zusammenrechnet.

$762k war der Durchschnitt deutscher Lösegeldzahlungen in den letzten 24 Monaten.

Die eigentlichen Kosten sind jedoch wesentlich **höher.**

Sie umfassen:

- Vorübergehende Schließung des Geschäftsbetriebes
- Reputationsverlust der Marke
- Umsatzeinbußen
- Rücktritte von Vorstandsmitgliedern
- Entlassungen

50% schätzen, dass ihr Unternehmen **Verluste von $1-10 Millionen** erlitten hat.

10% schätzen, dass ihr Unternehmen **Verluste von über $10 Millionen** erlitten hat.

99.5% aller deutschen Unternehmen **haben eine Cyberversicherung.**

Aber **nur** **32%** **sind sich sicher, dass diese auch Ransomware-Angriffe abdeckt.**

Nur **42%** derer, die einen Versicherungsanspruch geltend gemacht haben, **bekamen den Gesamtschaden zurückerstattet.**

Es ist schwer, sich effektiv vorzubereiten

Die meisten deutschen Unternehmen haben ihre Investitionen in die Cybersicherheit nach einem Sicherheitsverstoß erhöht, doch das Risiko ist damit nicht vollständig gebannt.

Nur ein Fünftel unserer Umfrageteilnehmer ist der Meinung, dass ihr Unternehmen **ausreichend auf den nächsten Angriff vorbereitet** sei.

96% **erhöhten die Ausgaben.**

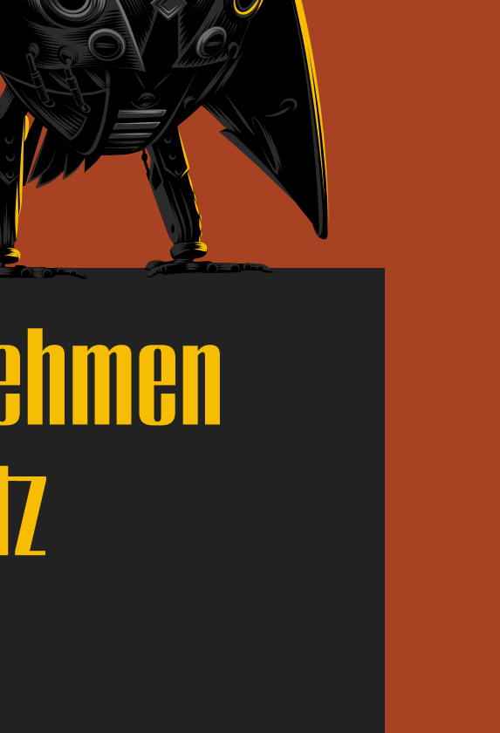
Doch **nur** **20%** glauben, dass sie **gut auf die Abwehr des nächsten Angriffs vorbereitet** sind.

Sie investieren in:

- Cybersicherheitsprofis
- Sensibilisierung der Mitarbeitenden
- Krypto-Wallets
- Neue Technologie (wie Endgerätesicherheit und Identitätsmanagementdienste)
- Bessere Compliance im eigenen Unternehmen der Lieferkette
- Cyberversicherungen

55% haben die **richtigen Leute**, aber nicht den richtigen Plan.

24% haben den **richtigen Plan**, aber nicht die richtigen Leute.



Weigern Sie sich, Lösegeld zu zahlen

Wenn Sie sich durch einen Ransomware-Angriff zur Zahlung eines sechsstelligen Lösegelds erpressen lassen, sind Ihre Probleme damit nicht unbedingt gelöst.

Denn das garantiert nicht, dass:

- Sie alle Ihre Systeme und Daten unbeschädigt zurückbekommen.
- Ihre Daten nicht auf dem Schwarzmarkt verkauft werden.
- Sie nicht erneut angegriffen werden.

Tatsächlich ist es leider sogar sehr wahrscheinlich, dass Sie erneut angegriffen werden.

Machen Sie Ihr Unternehmen mit KI-basiertem Schutz unantastbar

Cybereason ist von heutigen Angreifern bislang unbesiegt und auf zukünftige Herausforderungen vorbereitet.

Unsere starke Kombination aus Lösungen und Services bietet:

- Sicherheit rund um die Uhr
- Optimierte Sicherheitsprozesse
- Marktführende Geschwindigkeit bei Erkennung, Ersteinschätzung und Wiederherstellung

Lesen Sie den vollständigen Untersuchungsbericht

Lernen Sie aus den Erfahrungen von über 1000 Cybersicherheitsprofis in Unternehmen, die in den letzten 24 Monaten mindestens einen Ransomware-Angriff miterlebt haben.

Die Ergebnisse werden Sie überraschen.

Lesen Sie hier den vollständigen Untersuchungsbericht

Cybereason ist ein XDR-Unternehmen, das sich mit Partnern der ‚Defenders League' zusammentut, um Angriffe am Endpunkt, in der Cloud und im gesamten Ökosystem eines Unternehmens zu unterbinden. Die KI-gestützte Cybereason Defense Platform bietet branchenführende vorausschauende Präventions-, Erkennungs- und Abwehrfunktionen, die moderner Ransomware und fortschrittlichen Angriffstechniken stets einen Schritt voraus bleiben. Die Cybereason MalOpTM bietet unmittelbare kontextuelle Angriffsdaten zu jedem betroffenen Gerät, Benutzer und System – mit beispielloser Geschwindigkeit und Genauigkeit. Cybereason wandelt Bedrohungsdaten in praktische Entscheidungen um und hält mit dem Tempo Ihres Unternehmens mit. Cybereason ist ein privat geführtes internationales Unternehmen mit Hauptsitz in La Jolla, Kalifornien, das Kunden in mehr als 40 Ländern betreut."

cybereason