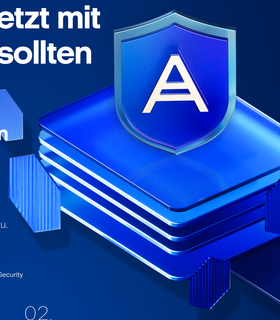
Die 5 wichtigsten Gründe, warum Sie Ihr Unternehmen jetzt mit EDR schützen sollten

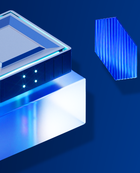
Acronis



01.
Erhöhte digitale Risiken erfordern einen präventiven Ansatz

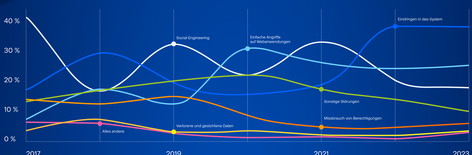
Die durchschnittlichen Kosten einer erreichten im Jahr 2023 mit 4,45 Mio. USD ein Rekordniveau. Dies entspricht einer Steigerung von 2,3 % gegenüber 2022.

Quelle: Cost of Data Breach Report, 2023, Ponemon Institute und IBM Security



02.
Schützen Sie sich vor raffinierten Angriffen

Die Angriffe werden immer raffinierter, und Sie brauchen entsprechend fortschrittliche Sicherheitskonzepte wie EDR, um sich davor zu schützen.



Quelle: Verizon Data Breach Investigation Report (DBIR) 2023

03.
Schnellere Reaktion auf Vorfälle und gründlichere Analyse

51 % der Unternehmen planen nach einem erlittenen Sicherheitsvorfall, ihre Investitionen in Sicherheit zu erhöhen. Zu den wichtigsten Bereichen, in die zusätzliche Investitionen getätigt werden sollten, gehören die Planung und das Testen der Reaktion auf Sicherheitsvorfälle (Incident Response – IR) , die Schulung der Mitarbeitenden sowie Technologien zur Erkennung von und Reaktion auf Bedrohungen.

Häufigste Investitionsarten unter denjenigen, die ihre Investitionen in die Sicherheit nach einem Sicherheitsvorfall erhöhen

Quelle: Cost of Data Breach Report, 2023, Ponemon Institute und IBM Security

04.
Einhaltung bestehender und künftiger rechtlicher Anforderungen

Jedes Unternehmen der Klasse A sollte Folgendes implementieren, es sei denn, der CISO hat der Verwendung angemessen gleichwertiger oder sicherer Ersatzmaßnahmen schriftlich zugestimmt: (1) eine Endpoint Detection and Response-Lösung zur Überwachung anomaler Aktivitäten, unter anderem auf sogenannte Lateral Movement-Bewegungsmuster von Angreifern hin.

Quelle: NY State DFS

Die drei größten Kostentreiber bei Sicherheitsverletzungenunter insgesamt 27 verschiedenen Faktoren.

Quelle: Cost of Data Breach Report, 2023, Ponemon Institute und IBM Security

05.
Anforderungen an Cybersicherheitsversicherungen

Quelle: Federal Trade Commission https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/cyber-insurance

Zu den Bewährten Verfahren gehören

- Verschlüsselung vertraulicher Daten
- Schwachstellenbewertung und Patch-Management
- EDR
- Planmäßiges Backup und ein DR-Plan
- Strenge Richtlinien für Authentifizierung (MFA) und Autorisierung (Least Privilege Management)
- Verhaltensbasierte Malware-Schutzfunktionen
- Schulungen zum Sicherheitsbewusstsein
- Incident Response Plan

Erleben Sie die ganzheitliche Cyber Protection, die die Resilienz Ihres Unternehmens gewährleistet

Jetzt kaufen | Jetzt testen