CryptoSpike

Ransomwareschutz und Zugriffstransparenz

VORTEILE

- **Proaktive Echtzeitüberwachung** diverser Indikatoren eines Angriffs
- **Blockieren** bekannter Bedrohungen, welche die Endpoint Protection passiert haben
- **Vollständige Datentransparenz** mit Rückverfolgbarkeit des Zugriffs auf Dateiebene
- **Punktgenaue Wiederherstellung** beschädigter Daten direkt aus dem Snapshot
- **Bereitstellung** in drei bis fünf Stunden, on-premise oder in der Cloud
- **Integration** in die bestehende SIEM-Plattform
- **Granulare Anpassung** der Monitoring-Richtlinien auf Volumen oder Abteilungsebene in real-time

*https://www.all-about-security.de/threats-und-co/alarmieren-der-anstieg-bei-ransomware-und-boesartigen-cyberangriffen-sowie-eine-verdopplung-der-bedrohungen-in-2021/

Ransomware ist ein globales Problem!

Ransomware-Angriffe steigen jährlich um über 100%, bereits über 600 Millionen Ransomwareattacken gab es weltweit allein im Jahr 2021.*
Das Resultat dieser Cyberangriffe sind lange Ausfälle der IT sowie hohe Kosten und Aufwände für die Wiederherstellung.

Backups schützen nicht ausreichend

- Backups schützen nicht vor Datendiebstahl
- Backups können kompromittiert oder gelöscht werden
- Ransomware schaltet oft zuerst die Backup Funktionen ab
- Komplette Wiederherstellung von Snapshots und Backups führt zu unnötigem Datenverlust

Endpoint Protection schützt nicht ausreichend

- Hacker nutzen innovative Formen von Phishing und Social Engineering um diese zu umgehen
- Firewalls und Endpoint Protection schützen nicht vor Insider Bedrohungen

CryptoSpike agentenloser Schutz

CryptoSpike ist eine Lösung zum Schutz von Dell PowerScale, Unity und PowerStore (ab CryptoSpike 3.3) vor Ransomware. Sie basiert auf vollständiger Zugriffstransparenz und schafft durch sofortige Alarmierung, automatisches User Blocking und granulare Restorefunktionen Abhilfe.

Die wichtigsten Schutzfunktionen sind:

Analyzer:
Datenzugriffe werden in Echtzeit gescannt und Anomalien sofort erkannt.

Blocklist: Anhand einer von ProLion zur Verfügung gestellten Liste, werden bei Ransomware typischen Dateiendungen die jeweiligen Benutzer blockiert.

User Blocking: Verdächtige User werden automatisch vom Zugriff auf sämtliche Daten ausgeschlossen.

File Restore: Ausschließlich korrumpierte Dateien werden wiederhergestellt, sämtliche weitere Daten bleiben unverändert.

Kontaktieren Sie uns

Unser hochqualifiziertes Team von Cybersecurity-Spezialisten freut sich darauf Sie zu beraten!
Treten Sie via E-Mail unter info@prolion.com mit uns in Kontakt.