VERITAS

#Ransomware Sind Sie geschützt?

DIE WACHSENDE BEDROHUNG

Ransomware hat sich schnell zu einer der gefährlichsten Cyber-Bedrohungen entwickelt. Sowohl Unternehmen als auch Verbraucher sind damit konfrontiert – und die weltweiten Verluste belaufen sich inzwischen wahrscheinlich auf Milliarden von Dollar pro Jahr. Veritas unterstützt Sie mit einer umfassenden Backup-Methode beim Schutz Ihrer Daten, egal wo diese gespeichert sind.

91 %
aller Cyberangriffe beginnen mit einer Spear-Phishing-E-Mail, einer bei Ransomware beliebten Taktik.[1]

71 %
der angegriffenen Unternehmen werden infiziert.[2]

10.000 USD
Lösegeldforderungen können bis zu 10.000 USD betragen, zahlbar in nicht nachverfolgbaren Bitcoins.[3]

GLOBALER SCHADEN DURCH RANSOMWARE

Für 2021 prognostizierter weltweiter Schaden durch Ransomware:

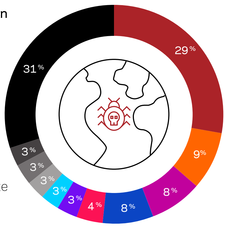
jährlich bis zu 20 Mrd. US-Dollar.[4]

Ransomware ist eine Bedrohung für alle gängigen Betriebssysteme:

iOS – Apple iOS™
Windows – Microsoft Windows™
Android™
Linux™

Ransomware-Infektionen nach Land[5]

Die USA sind nach wie vor das am stärksten von Ransomware-Angriffen betroffene Land. Sie sind möglicherweise deshalb ein so beliebtes Ziel, da Berichten zufolge 64 % aller Opfer das geforderte Lösegeld zahlen.

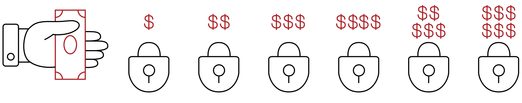


RANSOMWARE-ANGRIFFE SIND IMMER STÄRKER AUF DEM VORMARSCH[6]

DIE PREISFRAGE: SOLLTEN SIE BEZAHLEN?

Opfer eines Ransomware-Angriffs müssen sich bewusst sein, dass die Zahlung des Lösegelds NICHT immer den gewünschten Erfolg bringt. Manchmal fordern die Kriminellen nach Erhalt der Zahlung noch mehr Lösegeld. Wenn der Entschlüsselungsprozess schlecht implementiert ist, können dabei auch Dateien beschädigt werden. Und es kann noch schlimmer kommen:

20 % der Opfer, die ein Lösegeld bezahlen, erhalten nie einen Entschlüsselungscode.[7]



STEIGERN SIE IHRE RANSOMWARE-RESILIENZ

- Sichern Sie den physischen Zugriff auf den NetBackup-Produktionsserver bzw. die Appliance.
- Härten und schützen Sie die NetBackup-Masterserver.
- Sichern Sie Kommunikation und Ports.
- Schützen und sichern Sie Client-Knoten.
- Managen Sie Sicherheits-Patches und -warnungen.
- Testen Sie Ihren Disaster-Recovery-Plan.
- Erholen Sie sich von einem Datenleck.
- Führen Sie regelmäßig Sicherheitsaudits, Überprüfungen und Schulungen durch.
- Stellen Sie den Schutz kritischer Systeme für den Backup-Server sicher.

LADEN SIE DEN LEITFADEN HERUNTER

Lesen Sie unser Whitepaper und erfahren Sie, wie Sie in Ihrem Unternehmen einen robusten Plan für Ransomware Resiliency implementieren können

VERITAS

1. 91 % of cyberattacks begin with spear phishing email
2. Must-Know Ransomware Statistics 2018
3. Intermedia Ransomware 101: What your business needs to know about ransomware attacks
4. Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) By 2021
5. US remains the country most affected by ransomware
6. Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) By 2021
7. Why you should NOT pay ransom to malware creators

V0795 6/20