Wenn sich Ransomware ausbreitet, halten Sie Ihre Daten mit HPE StoreEver-Bändern sauber.

In den nächsten 40 Sekunden wird ein anderes Unternehmen zum Ziel eines Ransomware-Angriffs. Könnte es auch Ihres sein?

Nach Angaben des FBI zielt Ransomware alle 40 Sekunden auf ein Unternehmen ab, was eine vollständige Vermeidung fast unmöglich macht. Was können Sie also tun, um vorbereitet zu sein, wenn sich Ransomware in Ihrem Netzwerk ausbreitet? Der sicherste Ansatz könnte die Aufbewahrung einer Offline-Kopie Ihrer Daten auf LTO-Band sein. Inhalte auf Bandspeichermedien sind vom Netzwerk getrennt, was bedeutet, dass sie von Ransomware isoliert sind und nicht infiziert oder beschädigt werden können. Und um sich gegen alle Eventualitäten zu schützen, können Sie die integrierte AES-256-Verschlüsselung von LTO verwenden, falls die Bänder selbst gestohlen werden.

Ransomware ist die erste Art von Malware, die tatsächlich Einnahmen für den Angreifer generiert. Unternehmen, die von einer Ransomware-Attacke betroffen sind, müssen ein Lösegeld zahlen. Sobald Ihre Dateien infiziert sind, können Sie Tage, Wochen oder sogar Monate damit verbringen, das normale Geschäft wiederherzustellen.

Ransomware ist ein massives, heimtückisches Risiko für alle Unternehmen.
Die Angriffe häuften sich 2019 und trafen große Unternehmen und Regierungsbehörden, wodurch die öffentlichen Dienste lahmgelegt und größere Störungen verursacht wurden.

Jeder kann einen Ransomware-Angriff starten.
Es ist eine so erfolgreiche Geschäftsidee, dass Sie auf diese Weise Ihr eigenes Ransomware-Kit für nur 25 US-Dollar von der Stange bekommen könnten.

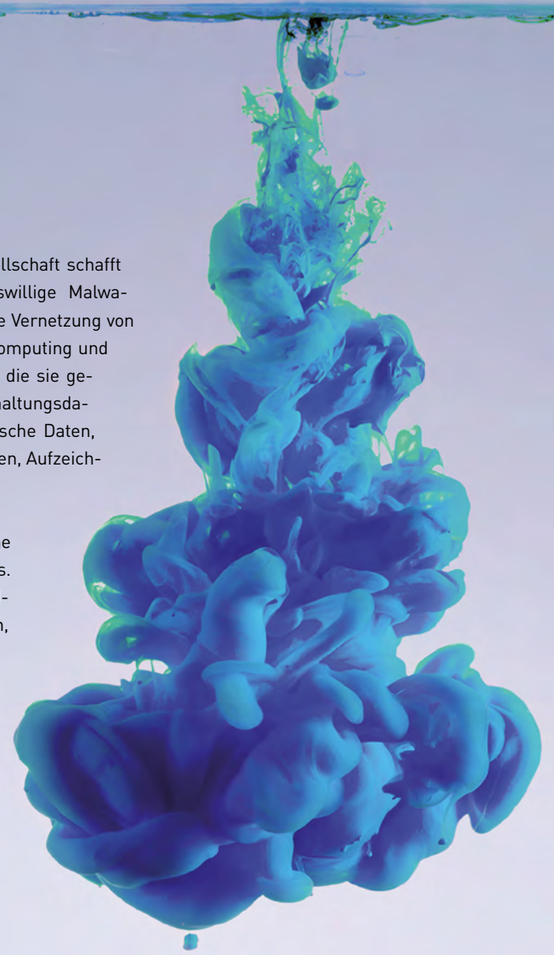
Ransomware-Angriffe kosten jedes Jahr mehrere Milliarden Dollar.
Für mittelständische Unternehmen sind es rund 713.000 US-Dollar. Die Lösegeldsumme stieg von 325 Millionen US-Dollar im Jahr 2015 auf unglaubliche 5 Milliarden US-Dollar im Jahr 2017. Bis Ende 2019 sollten sie voraussichtlich 11,5 Milliarden US-Dollar erreichen. 71% der von Ransomware-Angriffen betroffenen Unternehmen sind infiziert - das sind ungefähr drei von vier.

Es gibt alles zu verlieren. Ransomware bietet eine relativ einfache, kostengünstige und erfolgreiche Angriffsmethode für Kriminelle. Entweder zahlen sie das Lösegeld, weil sie unvorbereitet waren oder keine sicheren Backups erstellt haben, oder sie weigern sich, die Daten zu bezahlen und akzeptieren den Verlust insgesamt. Etwa jedes dritte betroffene Unternehmen verliert fünf Tage oder länger den Zugriff auf seine Daten. Selbst wenn Sie dafür bezahlen, ist der Preis für das Lösegeld nichts im Vergleich zu den Kosten, die durch Ausfallzeiten, Produktivitätsverlust und möglicherweise dauerhaften Verlust des Markenvertrauens entstehen.

Ransomware-Angriffe haben immer katastrophale Folgen, egal ob Sie eine Großstadt oder ein kleines ländliches Start-up sind.

Warum Jetzt?
Eine freie und offene digitale Gesellschaft schafft die perfekte Gelegenheit für böswillige Malware-Angreifer. Ransomware nutzt die Vernetzung von digitalen Netzwerken und Cloud-Computing und die Menge unstrukturierter Daten, die sie generieren, z. B. Medien- und Unterhaltungsdaten, Überwachungsdaten, geografische Daten, Audio- und Wetterdaten, Rechnungen, Aufzeichnungen, E-Mails und Sensordaten.

Ransomware mag eine Tatsache sein, mit der die Welt leben muss. Aber HPE StoreEver LTO-Bandspeichermedien können verhindern, dass Sie selbst betroffen sind.



Ihre Ansprechpartnerin

Kerstin Kullmann
Produktmanagerin für HPE
kerstin.kullmann@bechtle.com

Hewlett Packard Enterprise