Hewlett Packard Enterprise

GESCHÄFTSINHABER: SCHÜTZEN SIE IHR UNTERNEHMEN VOR RANSOMWARE, BEVOR ES ZU SPÄT IST!

FAKTEN ZU RANSOMWARE, DIE AUFHORCHEN LASSEN

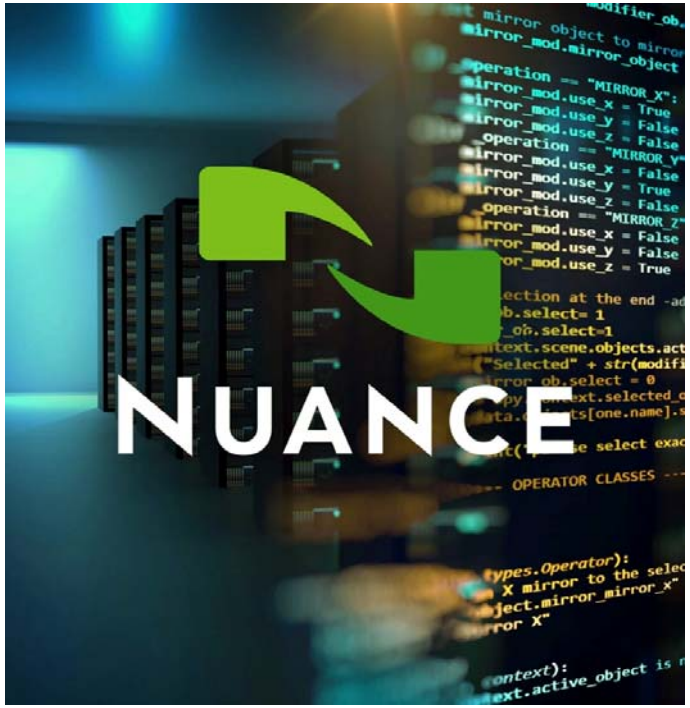
- Bis Ende 2019 wird vermutlich alle 14 Sekunden ein Unternehmen von Ransomware angegriffen worden sein. 2018 lag die Zahl noch bei 40 Sekunden.
- Anderen Statistiken zufolge wurden 71 % der von Ransomware betroffenen Unternehmen infiziert.
- Bei 50 % aller erfolgreichen Angriffe mit Ransomware werden mindestens 20 Computer eines Unternehmens infiziert.
- Angriffe mit Ransomware kosten mittelständische Unternehmen pro Vorfall durchschnittlich 713.000 USD.
- Zwischen 2015 und 2017 stiegen die Lösegeldforderungen von 325 Millionen USD auf 5 Milliarden USD. 2019 sollen sie bei 11,5 Milliarden USD gelegen haben.

RANSOMWARE IN AKTION

Die dänische Spedition Maersk erlitt einen Schaden von 300 Millionen USD durch Ausfälle während eines Ransomware-Angriffs. Zur Wiederherstellung des Systems,
die über 10 Tage dauerte, mussten bei Maersk 4000 Server, 45.000 PC und 2500 Programme neu installiert werden.

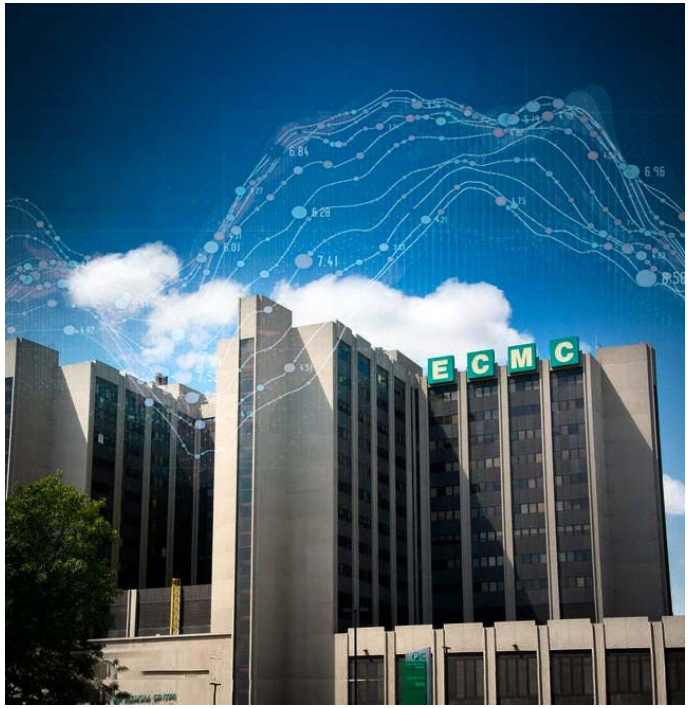
Das britische Pharmaunternehmen Reckitt Benckiser schätzt den durch Produktionsausfälle entstandenen Schaden durch einen NotPetya Ransomware-Angriff auf 140 Millionen USD.

RANSOMWARE IN AKTION



Der Technologieanbieter Nuance berichtete kürzlich, dass ein im Herbst 2017 erfolgter Ransomware-Angriff 68 Millionen USD an Rückzahlungen zur Folge hatte, die das Unternehmen seinen Kunden für Ausfälle leisten musste. Die Wiederherstellungskosten beliefen sich auf weitere 24 Millionen USD.

Der südkoreanische Netzbetreiber Nayana, Opfer eines WannaCry-Angriffs, zahlte 1 Million USD Lösegeld in Form von Bitcoins, um auf seine 150 Server wieder zugreifen
zu können und Web-Services für bis zu 3400 Kunden wiederherzustellen.



Im Krankenhaus Erie County Medical Center in New York fielen 6000 Computer aus. Als Folge musste 6 Wochen lang ohne Computer-Unterstützung gearbeitet werden. Die Wiederherstellung verschlang 10 Millionen USD.

RANSOMWARE IST EIN MILLIONENSCHWERES GESCHÄFT

Ransomware ist die erste Malware, mit der Angreifer etwas erwirtschaften. Von Ransomware angegriffene Unternehmen werden zu Lösegeldzahlungen von einigen Hundert bis zu mehreren Tausend Dollar erpresst, um schadhaft verschlüsselte Dateien wieder „freizuschalten“. Die Lösegeldforderungen reichen von 5.000 USD bis 50.000 USD oder, je nach Unternehmensgröße, sogar noch darüber hinaus.

EIN EINTRÄGLICHES GESCHÄFTSMODELL FÜR ANGREIFER

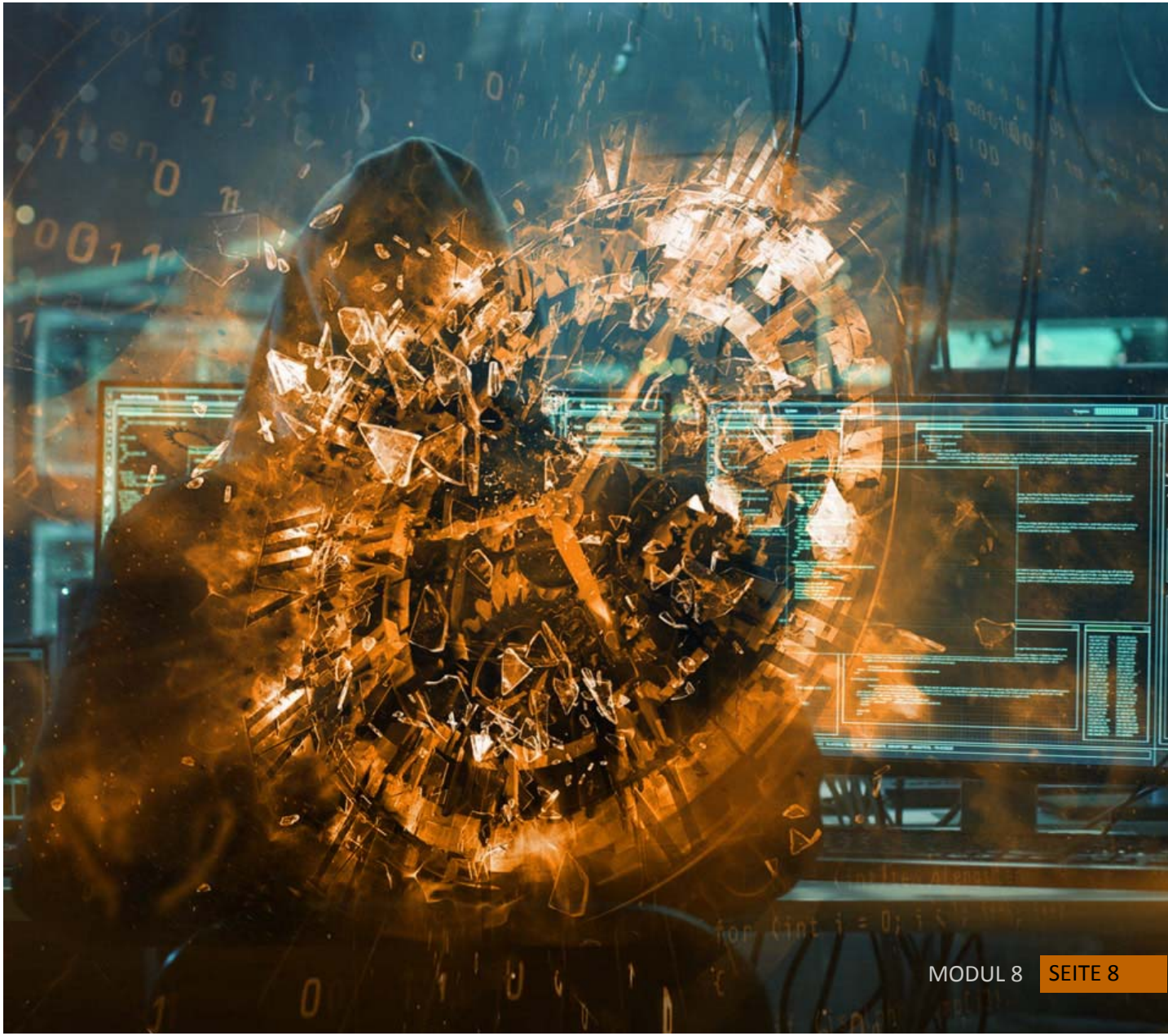
2019 schnellten die Angriffe mit Ransomware nach oben und legten große Unternehmen und Behörden lahm. Folge waren Versorgungsstörungen bis hin zum Komplettausfall. Über viele weitere Angriffe, besonders wenn sie nur kleine Betriebe betrafen, wurde gar nicht erst berichtet, was aber nicht bedeutet, dass der angerichtete Schaden nicht ebenso groß war.

EIN EINTRÄGLICHES GESCHÄFTSMODELL FÜR ANGREIFER

Ransomware als Dienstleistung ist mittlerweile Realität geworden. Kriminelle können vorgefertigte Ransomware-Sets für ihre Erpressungsversuche erwerben – zum Einstiegspreis von 25 USD.

EIN EINTRÄGLICHES GESCHÄFTSMODELL FÜR ANGREIFER

Selbst wenn Unternehmen auf Lösegeldforderungen eingehen (davon ist abzuraten), kann die Eingabe der Schlüssel zum Freischalten der Dateien Tage, wenn nicht gar Wochen dauern. Ca. 30 % der Unternehmen verloren mindestens 5 Tage lang Zugriff auf ihre Daten. Die Stadt Atlanta etwa brauchte für die Wiederherstellung sogar einige Wochen.



WIE KÖNNEN SICH INHABER VON UNTERNEHMEN ALSO SCHÜTZEN?

- Achten Sie darauf, dass Ihre Sicherheitssoftware immer auf dem aktuellen Stand ist.
- Achten Sie darauf, bei allen installierten Betriebssystemen stets die neueste Version zu verwenden. Installieren Sie Patches und Updates.
- Schulen Sie Endverbraucher.
- Nutzen Sie eine zuverlässige Datensicherung nach der 3-2-1-1-Regel.
- Nutzen Sie LTO Ultrium-Band zur Isolation (Air Gap).

WAS BESAGT DIE 3-2-1-1-REGEL UND WAS BEWIRKT SIE?

DREI KOPIEN IHRER DATEN

ZWEI VERSCHIEDENE MEDIENARTEN

EINE DAVON EXTERN AUFBEWAHRT

EINE DAVON OFFLINE ISOLIERT


RANSOMWARE-ANGRIFFE ERFOLGEN ALLE 40 SEKUNDEN
ISOLATION
Ransomware kann keine physikalische Isolation überwinden,
offline auf Band gespeicherte Daten sind sicher.

ES GEHT NICHT NUR UM RANSOMWARE

- Digitale Daten sind anfällig für alle Arten allgegenwärtiger Bedrohungen.
- Bandspeicherung ist nicht nur ein Gegengift gegen Ransomware.
- Durch mindestens eine Schutzvorrichtung werden Daten vor vielen Bedrohungen bewahrt.
- Nicht alle Datenausfälle werden von Schadprogrammen verursacht. Durch die isolierte, externe Sicherung Ihrer Daten beugen Sie Störungen durch Naturkatastrophen wie heftigen Stürmen, Überschwemmungen und Bränden vor.

LTO-VERSCHLÜSSELUNG – SIE HABEN DEN SCHLÜSSEL!

1. Bei einem Angriff mit Ransomware werden Ihre Daten von Kriminellen gekapert und verschlüsselt.

2. Eine LTO-Bandverschlüsselung macht es Angreifern nahezu unmöglich, Ihre Daten zu stehlen
   oder zu manipulieren.

3. Und des Beste daran ist: Sie haben den Schlüssel und damit die volle Kontrolle.