E-BOOK

datto

MSPeasy – Ransomware erfolgreich bekämpfen

Der MSPeasy-Guide, der Ihren Tag rettet

EINLEITUNG

Ransomware ist in den vergangenen Jahren ein großes Problem für Privatpersonen und Unternehmen geworden. Laut einer Studie des Sicherheitssoftware-Anbieters McAfee Labs wurden im zweiten Quartal des Jahres 2015 mehr als vier Millionen Ransomware-Samples identifiziert – darunter 1,2 Millionen neue. Im Vergleich dazu waren es im dritten Quartal 2013 weniger als 1,5 Millionen identifizierte Samples (400.000 neue).

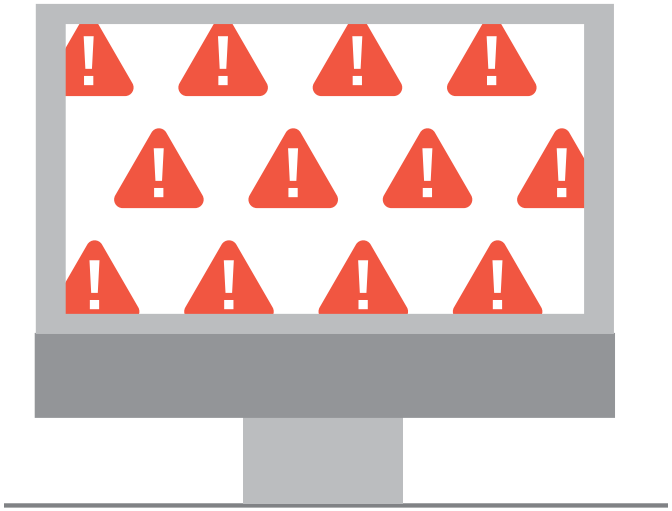
Ransomware-Attacken werden in nächster Zeit weder abklingen noch aufhören. Allein im ersten Quartal 2016 haben sich die Angriffe im Vergleich zum Gesamtjahr 2015 verzehnfacht und die Opfer mehr als 200 Millionen US-Dollar gekostet. Das Fazit: Ransomware ist eine Epidemie. Das Lösegeld ist zudem meist so niedrig, dass viele Opfer es einfach bezahlen und nur wenige Fälle strafrechtlich verfolgt werden. Das Lösegeld zu bezahlen, sollte jedoch in jedem Fall vermieden werden und es gibt effiziente Strategien, nicht in die Falle zu tappen. Ransomware ist also mehr denn je ein Thema, über das MSPs ihre Kunden aufklären sollten, um Best Practices und Lösungsansätze im Bereich Cyber-Sicherheit zu besprechen. Gleichzeitig bieten sich für MSPs Chancen für Neugeschäfte.

Dieses E-Book gibt Ihnen Informationen, welche Typen von Ransomware es derzeit gibt und wie sie sich ausbreiten. Sie erhalten praktische Ratschläge von MSPs und IT-Sicherheitsexperten, wie Sie Ihren Kunden das Risiko von Ransomware am besten kommunizieren können, damit diese die Bedeutung von Investitionen in Sicherheits-, Backup- und Recovery-Lösungen nachvollziehen können.

STATUS QUO UND UPDATE: RANSOMWARE

Hal Lonas, CTO des Sicherheitssoftware-Anbieters Webroot, bringt es auf den Punkt, weshalb Ransomware die Sicherheitslage auf den Kopf gestellt hat: „Früher wollten Kriminelle Daten, weil sie wertvoll für sie waren. Die Botschaft von Ransomware hingegen ist: ‚Deine Daten sind für mich nichts wert, aber wie viel sind sie Dir wert?' Das ist schon beängstigend clever."

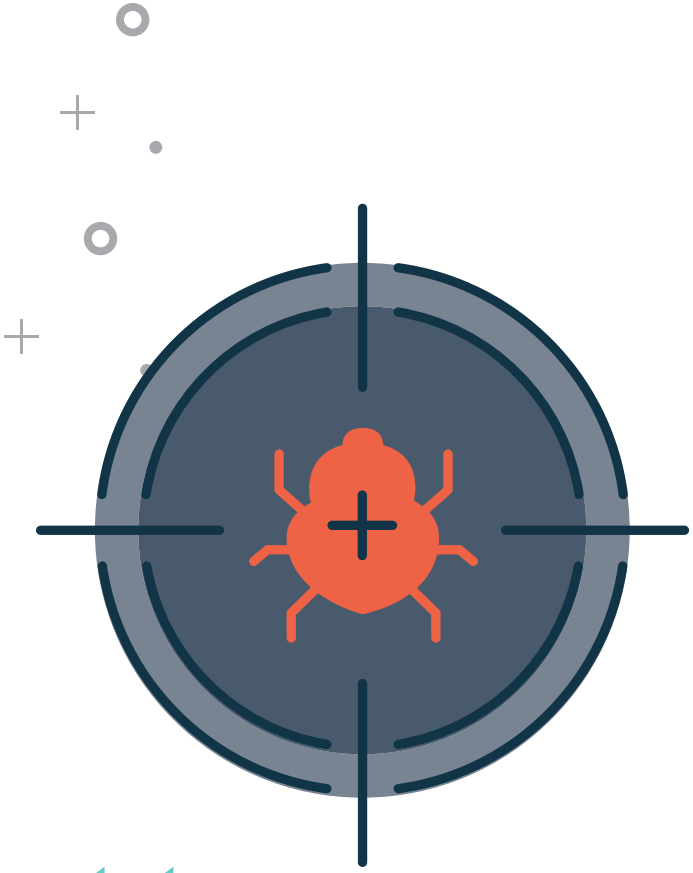
Früher wollten Kriminelle Daten, weil sie wertvoll für sie waren. Die Botschaft von Ransomware hingegen ist: „Deine Daten sind für mich nichts wert, aber wie viel sind sie Dir wert?" Das ist schon beängstigend clever.



Ransomware lässt sich in Gruppen einteilen. Jede Gruppe weist eigene Varianten auf. Im Laufe der Zeit werden immer neue Arten von Ransomware auftauchen, da Cyber-Erpresser den Ransomware-Code ständig verändern. Die gängigsten Abwehrtechnologien, wie z. B. Sicherheitssoftware, können diese dann nicht mehr erkennen. So haben wir z. B. einen Anstieg bei „polymorpher" Malware verzeichnet, einer Variante, die sich automatisch so verändert, dass jedes Endgerät mit einer scheinbar individuellen Malware infiziert wird. Dies ist ein großes Problem, da herkömmliche Sicherheits-software oft keine verschiedenen Varianten eines Stammes erkennen kann.

Die meisten Arten von Ransomware verwenden den AES-Algorithmus für die Verschlüsselung von Dateien. Um Dateien zu entschlüsseln, fordern Hacker dann meistens Zahlungen in Form von Bitcoins oder alternativen Online-Zahlungs-diensten. Die übliche Höhe des verlangten Lösegelds liegt bei etwa 500 US-Dollar. Viele Varianten (wie z. B. Jigsaw) drohen auch damit, dass das geforderte Löse-geld drastisch steigt, wenn nicht innerhalb eines Zeitfensters von 72 Stunden gezahlt wird. „Wir haben Ransomware-Attacken ganz unterschiedlichen Schweregrades erlebt ", so die Erfahrung eines MSPs.

E-Mail ist die häufigste Methode, um Ransomware zu streuen. Sie wird in der Regel über eine Art Social Engineering verbreitet; die Opfer werden dazu verleitet, einen E-Mail-Anhang herunterzuladen oder auf einen Link zu klicken. Sobald der



> Als MSP ist es wichtig, die neuesten Entwicklungen im Bereich Ransomware zu kennen und zu wissen, ob bestimmte Branchen ins Visier genommen werden. Je besser Sie informiert sind, desto effizienter können Sie die Daten Ihrer Kunden schützen.

Benutzer aktiv wird, installiert sich die Malware auf dem System und beginnt mit der Verschlüsselung von Dateien. Eine andere Strategie ist: Hacker installieren einen Code auf einer seriösen Website, der Computer-Benutzer auf eine andere, bösartige Website umleitet. Im Gegensatz zur SPAM-E-Mail-Methode sind also keine Aktionen des Opfers notwendig.

DIE WICHTIGSTEN AKTUELLEN RANSOMWARE-ARTEN

Als MSP ist es wichtig, die neuesten Entwicklungen im Bereich Ransomware zu kennen und zu wissen, ob bestimmte Branchen ins Visier genommen werden. Je mehr Informationen Sie haben, desto besser können Sie die Daten Ihrer Kunden schützen.
Es gibt eine Vielzahl von Ransomware-Typen, die sich heute stark ausbreiten.
Die Liste ist nicht vollständig, gibt Ihnen aber eine gute Übersicht, was Ihre Kunden attackieren könnte.

CryptoLocker

Ransomware gibt es seit über einem Jahrzehnt, sie wurde aber erst 2013 mit dem Aufkommen der Malware CryptoLocker richtig bekannt. Auch wenn das Original 2014 ausgeschaltet wurde, wurde der Ansatz vielfach kopiert. Und zwar so häufig, dass das Wort, CryptoLocker' mittlerweile als Synonym für Ransomware gebraucht wird.

Cerber

Cerber zielt auf Anwender des cloudbasierten Office 365 und soll mit einer aufwendigen Phishing-Kampagne Millionen von Anwender betroffen haben. Diese Art von Malware zeigt den wachsenden Bedarf an SaaS Backups zusätzlich zu den On-Premise-Backups.

CryptoWall

CryptoWall tauchte zum ersten Mal 2014 auf; mittlerweile gibt es Varianten mit unterschiedlichen Namen wie: Cryptorbit, CryptoDefense, CryptoWall 2.0 und CryptoWall 3.0.

KeRanger ist derzeit noch nicht weit verbreitet. Dennoch sollte man den Namen kennen, weil es die erste voll funktionsfähige Ransomware ist, die Mac-OS-X-Anwendungen sperrt.

Crysis

Diese neue Form von Ransomware kann Datenauf festen, Wechsel- und Netzlaufwerken verschlüsseln. Sie verwendet starke Verschlüsselung-Algorithmen und ein Schema, das es schwierig macht, diese Ransomware innerhalb einer kurzen Zeitspanne zu knacken.

CTB-Locker

Die Kriminellen, die diesen Stamm entwickelt haben, verfolgen einen anderen Ansatz bei der Verbreitung von Viren: Sie outsourcen den Infektionsprozess an Partner und geben hierfür einen Teil ihres Gewinns ab. Auf diese Weise verursacht die Malware viele Infektionen und generiert hohe Gewinne für die Hacker.

Jigsaw

Jigsaw verschlüsselt und löscht nach und nach Dateien, bis Lösegeld gezahlt wird. Die Ransomware löscht eine einzelne Datei nach der ersten Stunde, dann mehr und mehr pro Stunde bis zur 72-Stunden-Marke, bei der alle übrigen Dateien gelöscht werden.

KeRanger

KeRanger ist derzeit noch nicht weit verbreitet. Dennoch sollte man den Namen kennen, weil es die erste voll funktionsfähige Ransomware ist, die Mac OS X-Anwendungen sperrt.

LeChiffre

„Le Chiffre“ stammt vom französischen Substantiv „chiffrement“ ab (übersetzt „Verschlüsselung“). Und es ist der Name des Hauptschurken aus dem James-Bond-Roman „Casino Royale“, der Bonds Geliebte entführt, um ihn in eine Falle zu locken und sein Geld zu stehlen. Im Gegensatz zu anderen Varianten muss LeChiffre manuell auf dem System ausgeführt werden, das infiziert werden soll. Cyber-Kriminelle scannen automatisch Netzwerke nach schlecht gesicherten Remote Desktops, melden sich dort remote an und infizieren das Gerät manuell.

Dies könnte Sie auch interessieren:

Datto rettet Mittelständler vor IT-Katastrophe!

CASE STUDY

JETZT ANSEHEN

> Wahrscheinlich hat jeder unserer Kunden auf die eine oder andere Weise schon einmal Erfahrungen mit Ransomware gemacht. Aber viele wissen nicht genau, wie sie sich davor schützen sollen.

Locky

Locky wird in der Regel über eine als Rechnung getarnte E-Mail-Nachricht verbreitet. Beim Öffnen wird die Rechnung verschlüsselt und das Opfer angewiesen, Makros zum Lesen des Dokuments zu aktivieren. Wenn es Makros aktiviert, beginnt Locky, eine Vielzahl unterschiedlicher Dateitypen mithilfe von AES-Verschlüsselung zu chiffrieren. Die Spam-Kampagnen, über die Locky verbreitet wird, haben eine große Reichweite. Ein Unternehmen berichtete beispielsweise, innerhalb von zwei Tagen fünf Millionen E-Mails im Zusammenhang mit Locky-Kampagnen blockiert zu haben.

TeslaCrypt

TeslaCrypt verwendet ebenfalls einen AES-Algorithmus für die Verschlüsselung von Dateien. Diese Ransomware wird üblicherweise über das Angler-Exploit-Kit verbreitet und zielt auf Adobe-Schwachstellen ab. TeslaCrypt installiert sich selbst im Temp-Ordner von Microsoft. Wenn der Zeitpunkt gekommen ist, zu zahlen, hat das Opfer eine Auswahl an Zahlungsmöglichkeiten: Bitcoin, paysafecard und Ukash.

TorrentLocker

TorrentLocker ist nicht neu in der Malware-Szene, aber die Version von 2016 richtete mehr Zerstörung an als jede andere. Bei der Infektion verschlüsselt TorrentLocker nicht nur Daten, sondern sammelt auch E-Mail-Adressen aus dem Adressbuch des Opfers, um Malware über den infizierten Computer oder das infizierte Netzwerk hinaus zu verbreiten.

ZCryptor

ZCryptor ist ein sich selbstständig fortpflanzender Malware-Stamm, der ein wurm-artiges Verhalten zeigt, also Dateien verschlüsselt und auch externe Laufwerke und Flash-Laufwerke infiziert, sodass er auf andere Computer verteilt werden kann.

> Meist beginne ich das Gespräch so: ‚Ich möchte Sie nicht erschrecken oder beunruhigen, aber da ist etwas, worüber Sie nachdenken müssen.‘ Sprechen Sie das Thema einfach an. Es ist nicht schwer zu vermitteln – und nach dem Gespräch werden die Kunden das Problem schnell richtig einschätzen.

IHRE KUNDEN ÜBER RANSOMWARE AUFKLÄREN

„Wahrscheinlich hat jeder unserer Kunden schon einmal Erfahrungen mit Ransomware gemacht“, bestätigt ein MSP. „Aber viele wissen nicht genau, wie sie sich davor schützen sollen." Ransomware ist ein bekanntes Problem, aber viele Unternehmen wappnen sich noch nicht proaktiv – vor allem kleinere nicht. Das ist eine große Marktchance für MSPs.

Zum Beispiel bewerten viele Ransomware als reines Sicherheitsproblem. Aber das ist nicht ganz richtig. Da sich Ransomware ständig weiterentwickelt, ist es wichtig, den Kunden klar zu machen, dass sie ein Backup als zweiten Schutzschild benötigen, wenn Malware durch die Sicherheitslücken rutscht – was oft der Fall ist. Ransomware macht die Verbindung von Backup und Sicherheit unverzichtbar – beide Faktoren spielen eine wichtige Rolle für den Schutz eines Unternehmens. Als IT-Berater des Vertrauens sollten Sie Ihren Kunden folgenden dreigliedrigen Ansatz vermitteln: Eine effiziente Strategie zum Unternehmensschutz umfasst Aufklärung, Sicherheit und Backup.

Aufklärung

Ihre Kunden sollten über den Anstieg von Ransomware-Vorfällen Bescheid wissen und über Tools und eine Strategie verfügen, alle Mitarbeiter des Unternehmens zu informieren. Sinnvoll ist es, wenn Mitarbeiter an einer Cyber-Sicherheit-Schulung teilnehmen. Im Rahmen dieser Schulung sollten KMU bestimmte visuelle Beispiele zeigen, wie eine Phishing-E-Mail aussieht – eine der Hauptursachen für Ransomware-Infektionen. Alle Mitarbeiter sollten wissen, wie sie eine bösartige E-Mail erkennen, und genau wissen, was zu tun ist, wenn sie auf einen potenziellen Ransomware-Köder stoßen (d. h. keine Anhänge öffnen, Bescheid geben, wenn sie etwas sehen usw.). Dies ist ein wesentlicher Bestandteil des Schutzes Ihrer Kunden vor Angriffen und sollte heute in jedem Unternehmen grundlegende Praxis sein.

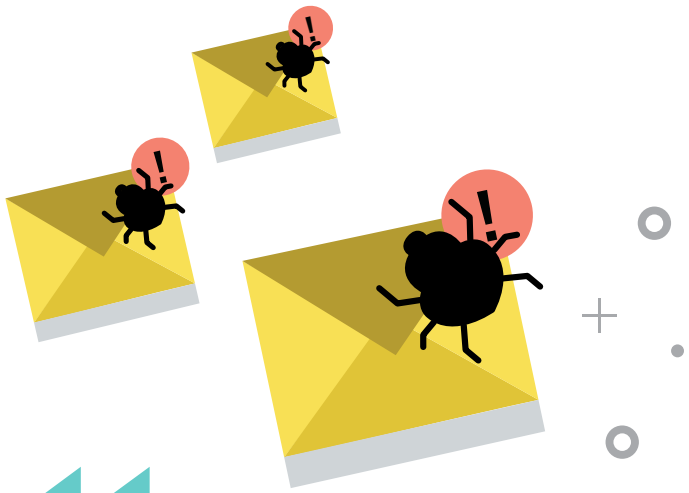
Ein IT-Dienstleister, der in den letzten zwei Jahren viele Ransomware-Infektionen erlebt hat, bestätigt: „Angesichts der Geschwindigkeit, mit der heute gearbeitet wird, ist es wirklich schwer, die Leute zu bremsen und sie dafür zu sensibilisieren, was sie anklicken. Vor allem, wenn Social Engineering durch Ransomware so clever gemacht ist." Das Unternehmen erläutert seinen Kunden die wichtigsten Ransomware-Statistiken und leitet dann zu dem Thema über, welche Technik notwendig ist. „Meist beginne ich das Gespräch so: ‚Ich möchte Sie nicht erschrecken oder beunruhigen, aber da ist etwas, worüber Sie nachdenken müssen.' Sprechen Sie das Thema einfach an. Es ist nicht schwer zu vermitteln – und nach dem Gespräch werden die Kunden das Problem schnell verstehen."

Sicherheit

Wenn es darum geht, Systeme vor Ransomware zu schützen, ist Antiviren-Software für jedes Unternehmen unverzichtbar. Firewalls und Web-Filterung sind ebenfalls ein Muss. Die meisten Sicherheitsanbieter empfehlen diesen mehrstufigen Ansatz zum Schutz vor Ransomware und auch Ihren Kunden wird das vermutlich einleuchten. Was ihnen aber wahrscheinlich nicht bewusst ist: Auch diese Maßnahmen bieten keinen hundertprozentigen Schutz.

MSPs sollten mit ihren Kunden auch darüber sprechen, wie wichtig es ist, die gesamte Software gepatcht und auf dem neuesten Stand zu halten, um das Unternehmen vor neu auftretenden Bedrohungen zu schützen. Stellen Sie auch sicher, dass Ihre Kunden die Notwendigkeit eines zusätzlichen Schutzschilds verstehen.

Es ist nämlich gar nicht selten der Fall, dass Ransomware die ersten Verteidigungslinien durchbricht. Erläutern Sie Ihren Kunden, dass es selbst bei diesen proaktiven Sicherheitsmaßnahmen immer noch Lücken geben kann. Und hier setzt eine Backup- und Recovery-Lösung an.



Stellen Sie auch sicher, dass Ihre Kunden die Notwendigkeit eines zusätzlichen Schutzschilds verstehen. Es ist nämlich gar nicht selten der Fall, dass Ransomware die ersten Verteidigungslinien durchbricht. Erläutern Sie Ihren Kunden, dass es selbst bei diesen proaktiven Sicherheitsmaßnahmen immer noch Lücken geben kann. Und hier setzt eine Backup- & Recovery-Lösung an.

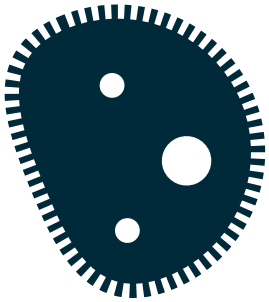
Backup

Moderne umfassende Lösungen zur Datensicherheit wie Datto erstellen in Abständen von nur fünf Minuten Snapshot-basierte, inkrementelle Backups und somit eine Reihe von Recovery Points. Dadurch ermöglichen sie es Unternehmen, Anwendungen aus Sicherheitskopien virtueller Maschinen auszuführen. Auch wenn Ihre Kunden sich vielleicht nicht für technische Details interessieren: Die Vorteile (und die Sicherheit!), die ihnen eine Lösung wie Datto bieten kann, werden Sie auf jeden Fall interessieren.

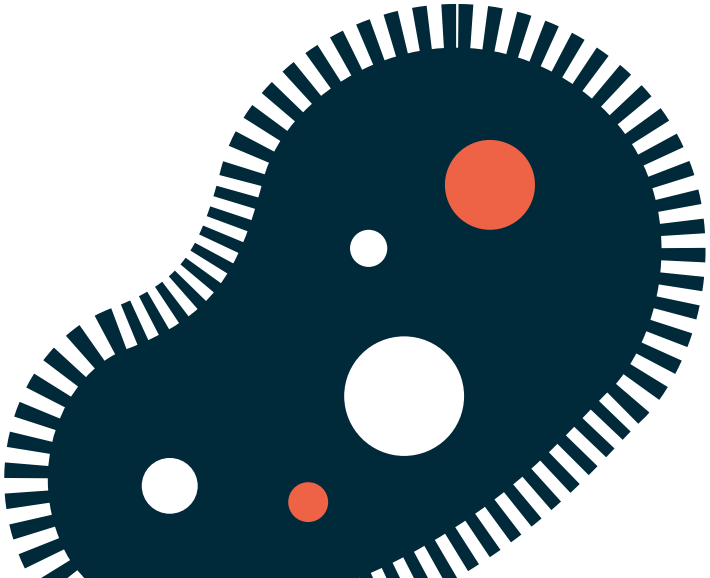
Konzentrieren Sie sich dabei vor allem auf die Vorteile von Datto und nicht primär auf die technologischen Funktionen und Innovationen. Wenn es um die Bedrohung durch Ransomware geht, liegen die Vorteile einer Data Protection-Lösung wie Datto in drei Bereichen:

1. Ihr Unternehmen muss Hackern nie Lösegeld zahlen, um kritische Daten zurückzubekommen.
2. Ihr Unternehmen vermeidet Datenverluste – durch Ransomware oder Ähnliches – da Backups häufig erstellt und schnell wiederhergestellt werden können.
3. Ihr Unternehmen wird keine signifikanten Ausfallzeiten haben (Benutzer können während der Wiederherstellung von Primärsystemen auf wichtige Daten und Anwendungen zugreifen).

„Wenn es um Disaster Recovery geht, ist nicht höhere Gewalt die größte Bedrohung. Sondern, dass jemand ein infiziertes Dokument öffnet“, betont ein MSP. „Dies ist zu einem Eckpfeiler der Diskussion über BCDR geworden. Unternehmer denken oft nicht über das Thema nach, aber das ändert sich langsam. Ransomware spielt hier eine unrühmliche Rolle. Die Leute fangen an, diese Bedrohung wirklich ernst zu nehmen.“



„Wenn es um Disaster Recovery geht, ist nicht höhere Gewalt die größte Bedrohung. Sondern, dass jemand ein infiziertes Dokument öffnet. Unternehmen denken oft nicht über das Thema nach. Aber das ändert sich langsam. Die Leute fangen an, die Bedrohung ernst zu nehmen."



Dies liegt vor allem daran, dass in letzter Zeit in den Nachrichten über eine Reihe spektakulärer Beispiele von Ransomware berichtet wurde, wie zum Beispiel einen Angriff auf ein kalifornisches Krankenhaus, bei dem Cyber-Erpresser ein Lösegeld von 17.000 US-Dollar erbeuteten. Das ist natürlich ein extrem hohes Lösegeld, aber es zeigt die Notwendigkeit eines Schutzes und ist ein geeigneter Aufhänger für Gespräche über Cyber-Erpressung.

Einige Partner von Datto verkaufen Backup-Optionen von Datto und andere, die günstiger sind. Sie empfehlen allerdings Datto, weil es den Kunden erlaubt, schneller wieder online zu gehen als mit anderen Backup Tools. „Es ist nicht schwierig, den Kunden zu überzeugen, wenn man den Kontext erläutert", sagt ein Partner von Datto. „Stellen Sie sicher, dass Kunden verstehen, dass Ausfallzeiten mit entgangenen Einnahmen gleichzusetzen sind. Und wenn Kunden Bedenken haben wegen der Kosten, vergleichen Sie die entgangenen Einnahmen mit den Kosten der Lösung."

Ein weiterer Partner von Datto bestätigt, dass es wichtig sei, den Kunden zu erläutern, weshalb sie die teurere Lösung nehmen sollten: „Zum Beispiel so: ‚Schauen Sie, ich kann die Einrichtung für Sie in wenigen Minuten vornehmen, bei der günstigeren Lösung würde das viel länger dauern, und das bedeutet mehr entgangene Einnahmen'. Es geht nicht darum, die Kunden unter Druck zu setzen, aber man sollte ihnen die Fakten zu der jeweiligen Lösung bewusst machen, damit sie die richtige Entscheidung treffen können."

RANSOMWARE IN ZAHLEN

Wenn Kunden nicht bewusst ist, wie real die Bedrohung durch Ransomware ist, können Sie einige wichtige Statistiken präsentieren. Hier sind fünf Fakten für das Gespräch mit zögerlichen Kunden:

> 97 % der heutigen Malware kann sich so verändern, dass jedes Gerät von einer individuellen Version angegriffen wird – was herkömmliche, signaturbasierte Sicherheitslösungen praktisch unbrauchbar macht.

1. Allein in den ersten drei Monaten des Jahres 2016 haben sich die Angriffe gegenüber dem Gesamtjahr 2015 verzehnfacht und laut FBI die Opfer mehr als 200 Millionen US-Dollar gekostet. Da Ransomware-Angriffe oft nicht gemeldet werden, liegt die Dunkelziffer vermutlich weit höher.

2. In den Jahren 2014 bis 2015 wurden etwa 27.000 Nutzer in Unternehmen angegriffen. In den Jahren 2015 und 2016 stieg diese Zahl auf 158.000. Der Hintergrund war laut Sicherheitsanbieter Kaspersky Labs, dass es sich Unternehmen leisten konnten, höhere Lösegelder zu bezahlen, und einen kompletten Verlust ihrer Systeme nicht in Kauf nehmen wollen.

3. Laut Webroot können sich 97 % der heutigen Malware so verändern, dass jedes Gerät von einer individuellen Version angegriffen wird – was herkömmliche, signaturbasierte Sicherheit praktisch unbrauchbar macht. Backups sind deshalb umso notwendiger.

4. Webroot berichtete außerdem, dass im Jahr 2015 täglich 100.000 neue bösartige IP-Adressen erstellt wurden. Im Jahr 2014 waren es noch 85.000 pro Tag, was darauf hindeutet, dass Cyber-Kriminelle immer neue IPs generieren, um nicht erkannt zu werden.

5. Laut PhishMe, einem Anbieter von Sicherheits-Management-Lösungen, war in den ersten drei Monaten des Jahres 2016 ein Anstieg bei Phishing-E-Mails um 6,3 Millionen zu verzeichnen. Dieser war in erster Linie auf einen plötzlichen Anstieg bei Ransomware zurückzuführen – einem Anstieg um 789 % im Vergleich zum vorigen Quartal.

> Ransomware-Angriffe erfolgen mit zunehmender Regelmäßigkeit – der Trend geht nach oben. Das ist ein großes Problem, aber es ist auch eine große Chance, Kunden aufzuklären und ihnen die Tools an die Hand zu geben, die sie zum Schutz ihrer Daten benötigen.

FAZIT

Der Schutz vor Ransomware passt genau zum proaktiven Ansatz von MSPs für das Monitoring und das Management von IT-Umgebungen ihrer Kunden. Backup- und Sicherheitstools, die sich problemlos in Remote Management- und Automation-Software integrieren lassen, erleichtern diese Aufgabe sehr.

Aus diesem Grund bestätigen unsere Partner, dass sie zwar eine Vielzahl von Backup- und Sicherheitslösungen unterstützen können, aber versuchen, so viel wie möglich zu standardisieren. Zum Beispiel sagt einer unserer Partner, dass er die Sicherheitssoftware von Trend Micro aufgrund der Integration in die von ihm verwendete PSA-Software von Autotask empfiehlt.

„Ransomware-Angriffe erfolgen mit zunehmender Regelmäßigkeit – der Trend geht nach oben“, sagt ein Datto Partner. „Das ist ein großes Problem, aber es ist auch eine große Chance, Kunden aufzuklären und ihnen die Tools an die Hand zu geben, die sie zum Schutz ihrer Daten benötigen.“