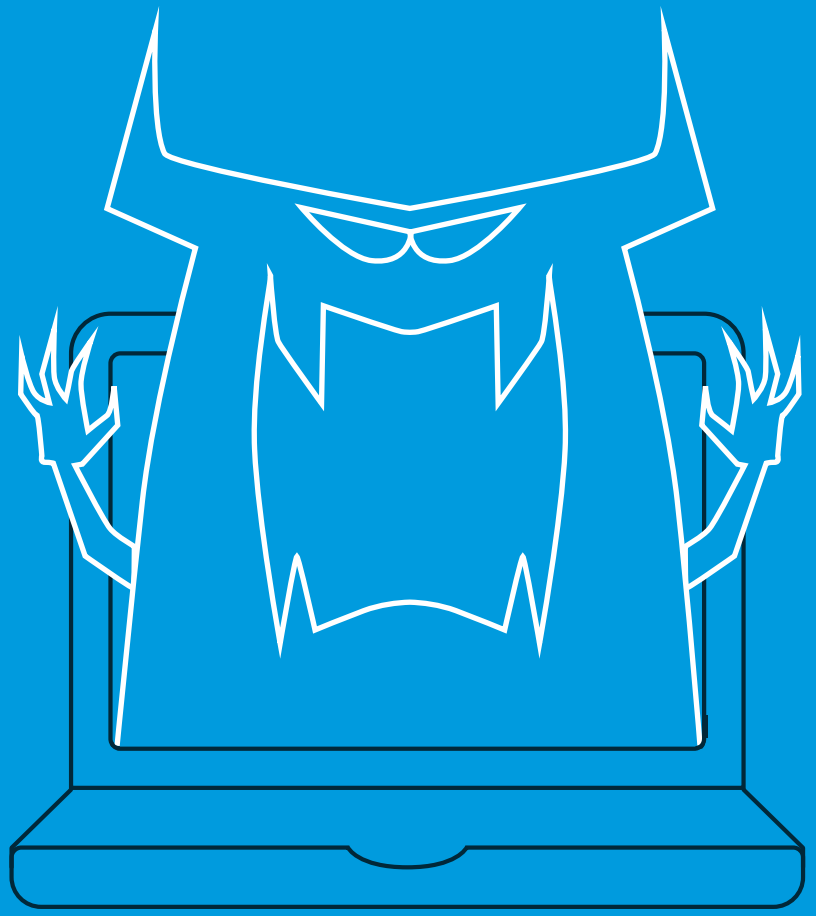
datto

eBook

DER RANSOMWARE-RATGEBER FÜR UNTERNEHMEN

Alles, was Sie wissen müssen, um Ihr Unternehmen optimal zu schützen



logiphys//IT
enabling your tomorrow

Inhalt

EINFÜHRUNG

Privatpersonen und Unternehmen werden zunehmend von Ransomware bedroht. Ransomware ist eine Art Malware, die Daten auf infizierten Systemen verschlüsselt. Für Cyber-Erpresser ist sie zu einer lukrativen Masche geworden. Die Malware sperrt Dateien der Opfer. Die Kriminellen fordern dann eine Zahlung, damit die Daten wieder freigegeben werden.

Ransomware-Attacken sind mittlerweile so häufig und umfangreich, dass sie es immer wieder in die Nachrichten schaffen. Unternehmen jeder Branche und Größe sind betroffen, wobei kleine Unternehmen besonders anfällig sind. Und Ransomware tritt immer häufiger auf. Im Datto Lagebericht zu Ransomware wurde festgestellt, dass schätzungsweise fünf Prozent aller KMU weltweit Opfer eines Ransomware-Angriffs wurden. 97 Prozent der MSPs gaben an, dass die Häufigkeit von Ransomware-Angriffen 2017 definitiv zugenommen hat. Ransomware verbreitet sich auf unterschiedlichste Weise und es entwickeln sich ständig neue Varianten.

Ihre Daten und Systeme lassen sich dennoch schützen – mit den richtigen Methoden. In diesem eBook erfahren Sie, wie die Malware verbreitet wird, welche verschiedenen Arten von Ransomware aktiv sind und was Sie tun können, um einen Angriff abzuwehren. Es hilft nicht, wenn Sie den Kopf in den Sand stecken, denn die Lösegeldjäger von heute spielen ein perfides Spiel. Darauf sollte Ihr Unternehmen vorbereitet sein.

Das Angler-Exploit-Kit nutzt HTML und JavaScript, um den Browser und die installierten Plug-ins des Opfers zu identifizieren. Dadurch kann der Hacker den Angriff wählen, der am erfolgreichsten ist. Angler nutzt verschiedene Techniken zur Tarnung und entwickelt sich kontinuierlich weiter, um von der Sicherheitssoftware nicht erkannt zu werden.

RANSOMWARE HEUTE

Ransomware lässt sich in verschiedene Varianten unterteilen. Es ist davon auszugehen, dass im Laufe der Zeit immer neue Stämme auftauchen werden. In der Vergangenheit waren Microsoft-Office-, Adobe-PDF- und Bilddateien das primäre Ziel. Laut Prognosen von McAfee werden in Zukunft aber auch andere Dateiarten ins Visier genommen, weil sich die Viren kontinuierlich weiterentwickeln.

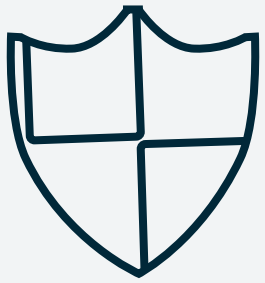
Die meisten Arten von Ransomware nutzen den AES-Algorithmus für die Verschlüsselung von Dateien; es kommen aber auch alternative Algorithmen zur Anwendung. Um Dateien zu entschlüsseln, fordern Hacker üblicherweise Zahlungen in Form von Bitcoins oder Online-Zahlungsdiensten wie Ukash oder paysafecard. Der übliche Preis liegt bei etwa 500 EUR, aber es wurden auch schon höhere Zahlungen verlangt. Die hinter Ransomware-Attacken stehenden Cyber-Kriminellen konzentrieren ihre Angriffe häufig auf wohlhabende Länder und Städte, sodass die Wahrscheinlichkeit höher ist, dass Opfer und Unternehmen das Lösegeld bezahlen.

So wird Ransomware verbreitet

Spam ist die häufigste Methode für die Verbreitung von Ransomware. Spam wird in der Regel über eine Art von Social Engineering verbreitet; die Opfer werden dazu verleitet, einen eMail-Anhang herunterzuladen oder auf einen Link zu klicken. Fake eMails können aussehen wie eine Mitteilung von einem Freund oder Kollegen, in der der Nutzer beispielsweise gebeten wird, sich einen Dateianhang anzusehen. Oder die eMail kommt von einer vermeintlich vertrauenswürdigen Institution (wie einer Bank) und Sie werden gebeten, eine Routine-Aufgabe zu erledigen. In anderen Fällen möchte Ransomware beim Empfänger Panik verbreiten. Es wird zum Beispiel behauptet, dass der Computer für illegale Aktivitäten genutzt worden sei. Sobald der Benutzer aktiv wird, installiert sich die Malware auf dem System und beginnt mit der Verschlüsselung von Dateien. Das kann in Sekundenschnelle mit einem einzigen Klick passieren.

Eine weitere gängige Methode für die Verbreitung von Ransomware ist ein Softwarepaket, auch „Exploit Kit“ genannt. Diese Pakete sollen Schwachstellen finden und sie für die Installation von Ransomware ausnutzen. Bei diesem Angriff installieren Hacker auf einer seriösen Website einen Code, der Computerbenutzer auf eine bösartige Website umleitet. Im Gegensatz zur Spam-Methode erfordert dieser Ansatz manchmal kein zusätzliches Handeln des Opfers. Dies wird auch „Drive-by-Download“-Angriff genannt.

Ein weitverbreitetes Exploit Kit nennt sich Angler. Eine vom Sicherheitssoftware-Anbieter Sophos durchgeführte Studie ergab, dass jeden Tag Tausende Websites erstellt werden, die Angler ausführen. Das Angler-Exploit-Kit nutzt HTML und JavaScript, um den Browser und die installierten Plug-ins des Opfers zu identifizieren. Dadurch kann der Hacker den Angriff



Auch Hacker mit geringen Computerkenntnissen können solche Kits anwenden. Laut McAfee gibt es Ransomware-as-a-Service-Angebote, die im Tor-Netzwerk gehostet werden und es praktisch jedem ermöglichen, solche Angriffe zu starten.

wählen, der am erfolgsreichsten ist. Angler nutzt verschiedene Techniken zur Tarnung und entwickelt sich kontinuierlich weiter, um von der Sicherheitssoftware nicht erkannt zu werden. Angler ist nur ein Exploit Kit unter vielen, die jeden Tag Schaden anrichten.

Spam-Botnets und Exploit Kits erfordern ein höheres Maß an technischem Können. Aber auch Hacker mit geringen Computerkenntnissen können solche Kits anwenden. Laut McAfee gibt es Ransomware-as-a-Service-Angebote, die im Tor-Netzwerk gehostet werden und es praktisch jedem ermöglichen, solche Angriffe zu starten.

HÄUFIGE VARIANTEN VON RANSOMWARE

Ransomware entwickelt sich kontinuierlich weiter. Es gibt ständig neue Varianten. Eine Liste aller Arten von Ransomware zu erstellen, die aktuell im Umlauf sind, ist quasi unmöglich. Die folgende Liste heutiger Ransomware ist deshalb auch nicht vollständig, gibt aber eine Übersicht über die wichtigsten Stämme und Arten.

CryptoLocker

Ransomware gibt es in der einen oder anderen Form schon seit zwei Jahrzehnten, aber CryptoLocker wurde 2013 zur greifbaren Chiffre für die Bedrohung durch Ransomware. Der ursprüngliche CryptoLocker-Botnet wurde im Mai 2014 ausgeschaltet, zuvor konnten Hacker aber fast drei Millionen US-Dollar von den Opfern erpressen. Seitdem wurde die CryptoLocker-Methode immer wieder kopiert, die heute aktiven Varianten haben aber nichts mehr mit dem Original zu tun. Der Begriff „CryptoLocker" ist zu einem Synonym für Ransomware geworden.

CryptoLocker wird über Exploit Kits und Spam verbreitet. Wenn die Malware ausgeführt wird, installiert sie sich selbst im Windows-Ordner „Benutzer" und verschlüsselt Dateien auf den Festplatten und verbundenen Netzlaufwerken. Sie dechiffriert nur Dateien mit bestimmten Erweiterungen, darunter Microsoft-Office-, OpenDocument-, Bild- und AutoCAD-Dateien. Auf dem Bildschirm des Nutzers erscheint dann eine Meldung, dass Dateien verschlüsselt wurden und eine Bitcoin-Zahlung verlangt wird.

CryptoWall

CryptoWall erlangte Berühmtheit, nachdem CryptoLocker ausgerottet wurde. CryptoWall erschien erstmals Anfang 2014 und mittlerweile sind Varianten mit unterschiedlichsten Namen aufgetaucht wie: CryptorBit, CryptoDefense, CryptoWall 2.0 und CryptoWall 3.0 usw. Wie CryptoLocker wird CryptoWall über Spam oder Exploit Kits verbreitet.

Die erste Version von CryptoWall nutzte einen öffentlichen RSA-Schlüssel, aber spätere Versionen verwenden einen privaten AES-Schlüssel, der mithilfe eines öffentlichen AES-Schlüssels zusätzlich getarnt wird. Wenn der Malware-Anhang geöffnet wird, kopiert

Locky ist eine relativ neue Art von Ransomware, aber die Methode ist bekannt. Die Malware verbreitet sich über Spam, oft durch eine als Rechnung getarnte eMail-Nachricht. Beim Öffnen wird die Rechnung verschlüsselt, und das Opfer angewiesen, Makros zum Lesen des Dokuments zu aktivieren.

sich die CryptoWall-Binärdatei in den Microsoft-Temp-Ordner und beginnt damit, Dateien zu verschlüsseln. CryptoWall verschlüsselt eine größere Anzahl von Dateitypen als CryptoLocker, folgt aber derselben Strategie: Nach der Verschlüsselung erscheint eine Lösegeldforderung auf dem Bildschirm des Benutzers.

CTB-Locker

Die Kriminellen, die sich hinter CTB-Locker verbergen, verfolgen einen anderen Ansatz der Virenverbreitung. Sie orientieren sich am Franchise-Prinzip und lagern den Infektionsprozess an Partner aus, die im Gegenzug einen Anteil am Gewinn erhalten. Das ist eine bewährte Strategie, um schneller ein hohes Volumen an Malware-Infektionen zu erreichen.

Wenn CTB-Locker ausgeführt wird, kopiert er sich selbst in das Microsoft-Temp-Verzeichnis. Anders als die meisten heutigen Formen von Ransomware nutzt CTB-Locker die Elliptic Curve Cryptography (ECC) für die Dateiverschlüsselung. CTB-Locker hat Auswirkungen auf mehr Dateitypen als CryptoLocker. Sobald die Dateien verschlüsselt sind, zeigt CTB-Locker eine Lösegeldforderung an, in der eine Zahlung in Bitcoins verlangt wird.

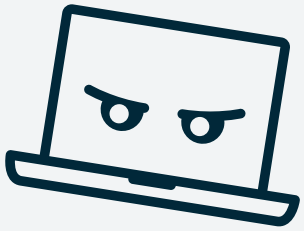
Locky

Locky verbreitet sich über Spam, oft durch eine als Rechnung getarnte eMail. Beim Öffnen wird die Rechnung verschlüsselt und das Opfer wird angewiesen, Makros zum Lesen des Dokuments zu aktivieren. Wenn Makros aktiviert werden, beginnt Locky, eine Vielzahl unterschiedlicher Dateitypen mithilfe von AES-Verschlüsselung zu verschlüsseln. Sobald die Verschlüsselung abgeschlossen ist, wird ein Lösegeld in Bitcoin verlangt. Erkennen Sie das Muster?

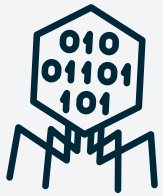
Die Spam-Kampagnen über Locky weisen ein neues Maß an Aggressivität auf. Ein Unternehmen berichtete, dass es innerhalb von zwei Tagen fünf Millionen eMails im Zusammenhang mit Locky-Kampagnen blockiert hat.

TeslaCrypt

TeslaCrypt ist ein weiterer Typ von Ransomware. Wie die meisten anderen Beispiele hier verwendet es den AES-Algorithmus für die Verschlüsselung von Dateien. Es wird üblicherweise über das Angler-Exploit-Kit verbreitet und greift speziell Adobe-Schwachstellen an. Sobald eine Schwachstelle ausgenutzt wurde, installiert sich TeslaCrypt selbst im Temp-Ordner von Microsoft. Wenn der Zeitpunkt gekommen ist, dass die Opfer bezahlen müssen, erhalten sie von TeslaCrypt verschiedene Zahlungsmöglichkeiten: Bitcoin, Paysafecard und Ukash.



Sicherheitssoftware ist ein Basisschutz, kann aber nicht alle Sicherheitslücken schließen. Der optimale Schutz vor Ransomware basiert auf drei Stufen: Aufklärung, IT-Sicherheit und Backup.



TorrentLocker

TorrentLocker wird üblicherweise über Spam-EMail-Kampagnen verbreitet und ist geografisch spezialisiert, d. h. eMails werden in eine bestimmte Region versandt. TorrentLocker wird häufig als CryptoLocker bezeichnet und nutzt einen AES-Algorithmus für die Verschlüsselung von Dateitypen. Neben der Verschlüsselung von Dateien sammelt er auch noch eMail-Adressen aus dem Adressbuch des Opfers, um Malware über den ursprünglich infizierten Computer/das ursprünglich infizierte Netzwerk hinaus zu verbreiten – das ist ein Alleinstellungsmerkmal vonTorrentLocker.

TorrentLocker verwendet die Technik „Process Hollowing“. Dabei wird ein Windows-Systemprozess im Standy-Modus gestartet, ein Schadcode installiert und der Prozess wieder aufgenommen. Für das Process Hollowing wird explorer.exe verwendet. Diese Malware löscht darüber hinaus Microsoft Volume Shadow-Kopien, um eine Wiederherstellung mithilfe von Microsoft-Datei-Recovery Tools zu verhindern. Auch hier ist Bitcoin die bevorzugte Währung für die Lösegeldzahlung.

KeRanger

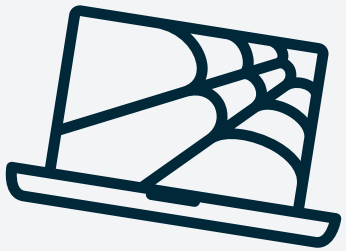
Laut ArsTechnica wurde die KeRanger Ransomware kürzlich in einem beliebten BitTorrent-Client entdeckt. KeRanger ist derzeit noch nicht weit verbreitet, aber erwähnenswert, da es die erste voll funktionsfähige Ransomware ist, die Mac-OS-X-Anwendungen sperren kann.

SCHUTZ VOR RANSOMWARE

Cyber-Kriminelle, die Ransomware einsetzen, sind ernst zu nehmende Gegner. Auch wenn kleine und mittlere Unternehmen bei Ransomware-Kampagnen nicht speziell ins Visier genommen werden, sind sie besonders gefährdet. Häufig haben die IT-Abteilungen nur wenige Mitarbeiter und setzen Technologien ein, die nicht mehr auf dem neuesten Stand sind: gute Voraussetzungen für einen erfolgreichen Ransomware-Angriff. Doch jedes Unternehmen, egal welcher Größe, kann sich vor Ransomware schützen. Sicherheitssoftware ist ein Basisschutz, kann aber nicht alle Sicherheitslücken schließen. Der optimale Schutz vor Ransomware basiert auf drei Stufen: Aufklärung, IT-Sicherheit und Backup.

Aufklärung: Aufklärung ist der erste Schritt, um Ihr Unternehmen vor Ransomware zu schützen. Es ist entscheidend, dass Ihre Mitarbeiter verstehen, was Ransomware ist und welche Risiken bestehen. Zeigen Sie Ihrem Team Beispiele verdächtiger eMails. Geben Sie Ihnen Anweisungen, was zu tun ist, wenn sie auf einen potenziellen Ransomware-Köder stoßen (d. h. keine Anhänge öffnen; melden, wenn sie eine verdächtige eMail erkennen usw.).

Da sich Ransomware jedoch ständig weiterentwickelt, kann auch die beste Sicherheitssoftware umgangen werden. Aus diesem Grund ist neben einer Anti-Viren-Software ein zweites Schutzschild für Unternehmen notwendig, um eine Wiederherstellung zu gewährleisten, sollte doch einmal eine Malware zuschlagen: Backup.



Führen Sie zweimal im Jahr eine Schulung durch, in der Sie Ihre Mitarbeiter über die Risiken von Ransomware und anderen Cyber-Bedrohungen aufklären. Bereiten Sie eine eMail vor, die Sie Mitarbeitern schicken, wenn diese neu ins Team kommen. Es ist wichtig, dass alle Mitarbeiter über Bedrohungen und Prävention direkt informiert werden. Halten Sie Ihr Team auf dem Laufenden, was Entwicklungen und aktuelle Ransomware-Varianten angeht.

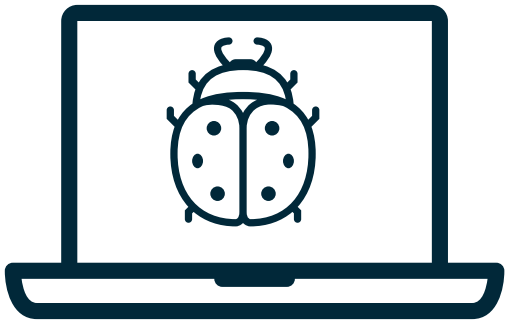
IT-Sicherheit: Anti-Viren-Software ist ein Muss für jedes Unternehmen. Achten Sie auch darauf, dass Ihre Sicherheitssoftware auf dem neuesten Stand ist, um die neuesten Typen von Malware zu erkennen und abzuwehren. Installieren Sie immer Patches und Updates von Unternehmensanwendungen, um Schwachstellen zu beseitigen.

Einige Anti-Viren-Softwareprodukte bieten Funktionen speziell gegen Ransomware. Sophos bietet beispielsweise eine Technologie, mit der Systeme auf bösartige Aktivitäten, wie die Änderung von Dateierweiterungen oder der Registry, gemonitort werden. Wenn Ransomware erkannt wird, kann die Software diese blockieren und den Benutzer benachrichtigen.

Da sich Ransomware jedoch ständig weiterentwickelt, kann auch die beste Sicherheitssoftware umgangen werden. Aus diesem Grund ist neben einer Antivirensoftware ein zweites Schutzschild für Unternehmen notwendig, um eine Wiederherstellung zu gewährleisten, sollte doch einmal eine Malware zuschlagen: Backup.

Backup: Moderne Total Data Protection-Lösungen wie Datto erstellen in Abständen von nur fünf Minuten Snapshot-basierte, inkrementelle Backups und somit eine Reihe von Recovery Points. Wenn Ihr Unternehmen Opfer eines Ransomware-Angriffs wird, können Sie mit dieser Technologie Ihre Daten auf einen Zeitpunkt vor dem Angriff zurücksetzen. Bei Ransomware hat das gleich zwei Vorteile: 1.) Ihr Unternehmen muss kein Lösegeld zahlen, um Ihre Daten zurückzubekommen. 2.) Sie können sicher sein, dass alle wiederhergestellten Daten und Dateien nicht von der Malware infiziert sind, da alle Inhalte aus dem Zeitraum vor einer Infektion wiederhergestellt wurden.

Darüber hinaus ermöglichen Lösungen zur Datensicherung es heute, Anwendungen von Image-basierten Backups virtueller Maschinen auszuführen. Diese Fähigkeit wird im Allgemeinen als „Recovery-in-Place“ oder „Instant Recovery“ bezeichnet. Diese Technologie kann auch bei der Wiederherstellung nach einem Ransomware-Angriff nützlich sein, da Sie damit den Betrieb ohne oder mit nur geringen Ausfallzeiten fortsetzen können, während Ihre primären Systeme wiederhergestellt werden. Die Datto Version dieser unternehmenskritischen Technologie wird Instant Virtualization genannt und virtualisiert Systeme innerhalb von Sekunden entweder lokal oder in einer sicheren Cloud. Durch diese Lösung ist der unterbrechungsfreie Betrieb des Unternehmens auch im Notfall gewährleistet.



FAZIT

Cyber-Erpresser, die Ransomware nutzen, sind für Unternehmen eine Bedrohung – von der Pizzeria bis zu großen Unternehmen. Aber durch Aufklärung und die richtigen Lösungen lässt sich das Risiko eines erfolgreichen Angriffs effizient reduzieren. Stellen Sie zum Beispiel sicher, dass Ihre Mitarbeiter wissen, was Ransomware ist und wie sie sich verbreitet. Unterschätzen Sie nicht die kriminelle Energie von Hackern: Sie verwenden viel Zeit und Energie darauf, Ransomware zu optimieren. Aus diesem Grund benötigen Sie erstklassige Sicherheitssoftware und Backups. Schützen Sie Ihr Unternehmen und schonen Sie Ihre Nerven.

Wissen, Schulungen und Sicherheitssoftware sind eine sinnvolle Strategie. Patch-Management ist zudem unerlässlich. Achten Sie darauf, dass Ihre Software aktuell und sicher ist. Wenn Ransomware dann doch alle Schutzmaßnahmen überwunden hat, ist es das Backup, das den Schaden behebt. Investieren Sie in ein modernes Backup-Produkt mit Features, die Downtime dauerhaft ausschließen.

Kontakt:

Tomke Overlander
Logiphys Datensysteme GmbH
Kuhnbergstrasse 27
73037 Göppingen