Whitepaper Erpressersoftware (Ransomware)

Hintergründe, wertvolle Tipps und massiv steigende Bedrohungen

ZYXEL

Your Networking Ally

Das Thema «Erpressersoftware (Ransomware)» beschäftigt die IT-Welt wie kein zweites.
Dieses Whitepaper enthält Hintergründe, Meinungen und Tipps zum Schutz vor den gefürchteten Trojanern.

Inhalt

Auch Fernseher betroffen

Nun also auch noch die Fernseher. Ein Smart-TV der Marke LG funktionierte plötzlich nicht mehr. Auf dem Bildschirm war die Mitteilung zu lesen, dass das Gerät nur dann wieder entsperrt wird, wenn 500 Dollar bezahlt werden.

Es ist nur eine von unzähligen Meldungen über Erpressersoftware (Ransomware). Kein anderes Thema sorgt derzeit in der IT-Branche für so viel Aufsehen. Betroffen sind in erster Linie Unternehmen. Gemäß einer Studie von IBM bezahlen 70 Prozent der Unternehmen das geforderte Lösegeld – die Hälfte davon mehr als 10 000 US-Dollar und 20 Prozent gar über 40 000 US-Dollar.

Tagtäglich entdeckt das BSI etwa 380.000 neue Schadprogrammvarianten. Dabei handelt es sich verstärkt um Erpressersoftware (Ransomware). Da keine Entwarnung in Sicht ist, sollten sich Unternehmen und Institutionen wappnen.

Was ist Erpressersoftware (Ransomware)?

Erpressersoftware (Ransomware) wird auch Verschlüsselungs- oder Erpressungstrojaner genannt. Die Schadsoftware (Malware) verschlüsselt Dateien auf dem Computer oder Smartphone des Opfers sowie häufig auch auf den verbundenen Netzlaufwerken. Die Daten werden damit unnutzbar. Dem Opfer zeigt die Erpressersoftware (Ransomware) danach einen Sperrbildschirm mit der Aufforderung an, eine bestimmte Summe (oft in Form von Bitcoins) an die Angreifer zu übermitteln. Nur dann würden die Dateien wieder entschlüsselt werden.

Über dieses Whitepaper

Dieses Whitepaper enthält Hintergründe, Meinungen und Tipps zum Schutz vor den gefürchteten Erpressungstrojanern. Es richtet sich gleichermassen an IT-Fachleute wie auch Privatanwender.

10 WERTVOLLE TIPPS

Was sollten IT-Administratoren und Mitarbeitende beachten, um sich gegen Erpressersoftware (Ransomware) wirkungsvoll zu schützen? Wir fassen die wichtigsten Tipps hier zusammen.

01 Backups! Backups! Backups!

Trotz aller nachfolgenden Maßnahmen ist ein Unternehmen nie komplett gegen Erpressersoftware (Ransomware) geschützt. Der wichtigste Tipp ist daher regelmäßige Backups. Zudem sollten die Backups unbedingt vom Netzwerk getrennt aufbewahrt werden. Ansonsten könnten auch die Sicherungen verschlüsselt werden.

02 Up-to-date

Ob Betriebssystem oder Office-Anwendungen – am sichersten sind jeweils die neuesten Versionen. Hersteller aktualisieren ihre neuesten Software-Versionen jeweils immer zuerst. Update für ältere Programme gibt es – wenn überhaupt – meist erst verspätet. Es empfiehlt sich daher, möglichst neue Software-Versionen zu nutzen und diese stets aktuell zu halten.

03 Unsichere Websites

Der Besuch unsicherer Websites sollte vermieden werden. Doch auch seriöse Portale können mit Schadsoftware verseucht sein. Besondere Vorsicht ist hierbei bei Blogs geboten – sie sind die am häufigsten infizierten Websites. Firewalls mit Schutzmechanismen erhöhen die Sicherheit beim Surfen. Insbesondere Content-Filter helfen, indem sie verseuchte Websites blockieren. Die entsprechenden Datenbanken werden ständig aktualisiert. So werden auch «frisch» infizierte Websites schnell gekennzeichnet und sind danach nicht mehr aufrufbar.

04 Besondere Vorsicht bei E-Mails

Trotz Spamfilter landen ständig E-Mails von unbekannten Absendern im Postfach. In diesen Fällen unbedingt misstrauisch sein – und vor allem keine Anhänge öffnen. Und Vorsicht: Die Tricks der Betrüger werden immer ausgefeilter. Ob fingierte und gut gemachte Bewerbungen oder echt aussehende Mails des Finanzdienstleisters – eine grundsätzliche Skepsis ist bei E-Mails stets angebracht.

05 Schutz durch Hard- und Software

Zu den wirkungsvollsten Schutzmechanismen zählen die Firewalls. Kombiniert mit verschiedenen Software-Lösungen bieten Firewalls einen umfassenden Schutz gegen Erpressersoftware (Ransomware) und andere Schadprogramme – vom Gateway bis zur Endpoint Protection (Client). SSL-Inspection, VPN, Application-Intelligence, Intrusion-Detection-Prevention, Single-Sign-On sowie Content-Filter sind heute gängige Funktionen einer Firewall. In Sachen Software sind zudem Antiviren-Lösungen und auch spezielle Anti-Ransomware-Programme sinnvoll. Wichtig ist, dass die Programme und Firewalls aufeinander abgestimmt werden, damit sich diese nicht gegenseitig beeinträchtigen.

06 Ohne Admin-Reche arbeiten

Die Benutzerprofile der Mitarbeitenden wenn möglich nicht mit Admin-Rechten ausstatten. Viele Programme können mit normalen Rechten nicht installiert werden. Genauso wird aber auch so manche Schadsoftware nicht installiert.

07 Skriptblocker einsetzen

Für den Webbrowser empfiehlt es sich, einen Skriptblocker zu installieren. Dieser verhindert das Ausführen von schädlichem Code auf Websites.

08 Mitarbeiter sensibilisieren

Die Mitarbeitenden sollten auf das Thema Erpressersoftware (Ransomware) aufmerksam gemacht werden. Auch sollte das richtige Verhalten im Ernstfall geschult werden. So können beispielsweise Fallstudien durchgespielt werden. Die Schulungen sollten in regelmäßigen Abständen wiederholt werden.

09 Vorbereitet sein

Planen, wie man im schlimmsten Fall vorgehen wird. Was ist zu tun? Wer sind die Ansprechpersonen für die Mitarbeitenden? Was passiert in der Zeit zwischen Infektion und vollständiger Wiederherstellung der Systeme? Ein geregelter Ablauf hilft, im Ernstfall die Ruhe zu bewahren.

10 Im Falle einer Infektion

Den betroffenen Computer sofort von allen Netzwerken trennen. Prüfen, ob weitere Computer im Netzwerk verseucht sind. Danach das System neu installieren und sämtliche Passwörter ändern. Nun das Backup einspielen. Es empfiehlt sich zusätzlich die lokalen Polizeibehörden einzuschalten und Anzeige zu erstatten. Lösegeld an die Erpresser zu bezahlen, ist nicht empfohlen. Es gibt keine Garantie, dass die verschlüsselten Daten danach auch wirklich entschlüsselt werden.

Schadsoftware im Netz

Das Internet ist Segen und Fluch zugleich. Die Gefahren werden aber oft nicht ernst genommen. Dabei nehmen die Fälle von Erpressersoftware (Ransomware) und anderen Schadprogrammen rasant zu.

Trojaner bei Bankgeschäften

Nur mal schnell eine Überweisung tätigen. Kaum jemand macht sich klar, welche massive Folgen ein Infekt mit Malware haben kann. Doch es passiert ständig. Die Newsletter sind voll mit Nachrichten über Trojaner, wobei die Banking Trojaner der Traum eines Kriminellen und der Albtraum eines jeden Nutzers sind. Der E-Banking Trojaner „Tordow" wurde in dem Zusammenhang im letzten Jahr auch als „Super-Trojaner" gekürt.

E-Banking Trojaner „Tordow"

Hatte sich Tordow einmal erfolgreich eingenistet, konnte der Trojaner zum Beispiel Anrufe mitschneiden, Bankinformationen kopieren und weitere Malware nachladen und installieren. Zudem bestand die Gefahr, dass der Schädling Zugangsdaten inklusive Passwörtern für Online-Dienste aus mobilen Webbrowsern auslesen konnte. Dies ist nur ein Beispiel für das enorme Schadenspotential, dem Nutzer ausgesetzt sind.

Vielzahl von Schadprogrammen

Neben Trojanern, die einen Computer ausspionieren und so etwa sensible Bankdaten an Dritte weiterleiten können, gibt es viele weitere Arten von Schadprogrammen. In letzter Zeit liest man in vielen Medien von Erpressersoftware (Ransomware). Diese wird auch Verschlüsselungstrojaner genannt und kennt einige Formen – der gemeinsame Nenner ist aber Erpressung.

So werden Daten auf dem Computer und auch den Netzlaufwerken des Opfers verschlüsselt – und erst bei einer Lösegeldzahlung wieder entschlüsselt. Das versprechen die Angreifer zumindest. Experten raten davon ab, in solchen Fällen Geld zu überweisen. Vielmehr raten sie zu regelmäßigen Backups, die getrennt von Computer und Netzwerk aufbewahrt werden sollten.

Preiswerte Firewalls mit Content-Filter

Die erwähnten Gefahren einfach hinzunehmen, ist jedoch nicht alternativlos. Denn für Privatpersonen wie auch für Unternehmen aller Größen gibt es heutzutage bezahlbare Lösungen für einen zuverlässigen Schutz vor Erpressersoftware (Ransomware) und anderen Schadprogrammen. So sind beispielsweise erschwingliche Firewalls mit Content-Filter- und weiteren Sicherheitsfunktionen erhältlich, die den Schutz deutlich erhöhen.

Eine breite Produktpalette an Firewalls bietet der Netzwerkspezialist Zyxel. Zyxel arbeitet im Bereich des Content-Filters mit Cyren zusammen. Cyren wiederum betreibt eine Datenbank, in welcher über 140 Millionen der relevantesten Websites laufend überprüft werden. Ist eine Website verseucht, wird dies in der Datenbank hinterlegt und die Zyxel-Firewall blockt ab diesem Zeitpunkt die entsprechende Internetadresse. Der Content-Filter sperrt also nicht einfach ganze Kategorien – er blockt in erster Linie gefährliche Websites.

Umfassender Schutz

Neben Content-Filter besitzen die Zyxel-Firewalls für Unternehmen noch weitere Funktionen, die zum Schutz beitragen. SSL-Inspection, VPN, Application-Intelligence sowie Intrusion-Detection-Prevention bieten gemeinsam eine umfassende Sicherheit.

Umfassende Hilfe zur Konfiguration einer Zyxel-Firewall bietet das Supportteam von Zyxel. Unsere Netzwerkexperten erklären Schritt für Schritt, wie die Firewall eingerichtet werden muss. Nach korrekter Konfiguration bietet das Produkt einen umfassenden Schutz vor unerwünschten Angriffen. Und der Nutzer kann mit deutlich weniger Sorgen seine Lieblings-Internetseiten aufrufen. ■

Ransomware verbreitet sich rasant – und dringt meist unbemerkt durch die Hintertür ein.

Düstere Aussichten

Das allgegenwärtige Thema Erpressersoftware (Ransomware) wird zu einem ernsten Problem. Die Experten Marc Henauer und Andreas Wisler zeichnen ein düsteres Bild.

Erschreckend viele Infektionen

5000 Infektionen pro Stunde – und das allein in Deutschland. Erpressersoftware (Ransomware) ist auf dem Vormarsch. Marc Henauer, Leiter der Sektion MELANI (Melde- und Analysestelle Informationssicherung) führt aus.

Neue Akteure

Mit der zunehmenden Bedeutung der IT für Geschäftsprozesse nehme auch die Möglichkeit für Betrug, Spionage und Erpressung zu, erklärte Henauer. Heute treten auch neue Akteure als die Bösen auf – die organisierte Kriminalität und sogar Staaten haben Erpressersoftware (Ransomware) für sich entdeckt. Neben kommerziellen Motiven werden so vermehrt auch der Aufbau von Know-how und politische Zwecke zu Gründen, weshalb Erpressersoftware eingesetzt wird. Wie ernst auch der Bund die Problematik nimmt, zeigt sich am Nationalen Ransomware-Awareness-Tag, den MELANI zuletzt am 19. Mai 2016 veranstaltet hat.

Kaffeemaschinen und Autos

Andreas Wisler trägt wenig zur allgemeinen Erleichterung bei. Der CEO der goSecurity GmbH kennt verschiedene Praxisfälle von Cyberattacken. Gehackte Kaffeemaschinen, lahmgelegte Krankenhäuser und ein Tesla, der nicht mehr starten will. Mit zunehmender Vernetzung werden auch Geräte fernab von Computern und Smartphones zu beliebten Angriffszielen.

Auch kleine Firmen betroffen

Wisler wies darauf hin, dass sich längst nicht mehr nur in großen Unternehmen die Fälle von Erpressersoftware (Ransomware) häufen. Auch kleine Betriebe und gar Ein-Mann-Firmen werden immer häufiger angegriffen. KMU waren im Jahr 2015 mit 43 Prozent die am meisten attackierten Unternehmen. Die gängige Meinung vieler KMU-Chefs, dass nur Großunternehmen durch Ransomware gefährdet sind, ist also definitiv falsch.

Schädliche Blogs

Die gefährlichsten Websites in Sachen Schadsoftware sind nicht etwa Seiten mit pornografischem Inhalt. Die meisten schädlichen Programme werden über Blogs verbreitet. Auch Onlineshops sind beliebte Tummelplätze für Kriminelle.

Ernüchterndes Fazit

Generell gilt: Die Chancen, Opfer von Erpressersoftware (Ransomware) zu werden, sind so hoch wie nie zuvor. Für Privatpersonen, Ein-Mann-Unternehmen, KMU und auch große Unternehmen bedeutet diese wachsende Gefahr vor allem eines: Im Internet vorsichtig sein, sich so gut wie möglich schützen und für den Fall der Fälle gut vorbereit sein. Tipps dazu sind auf der dritten Seite in diesem Whitepaper zu finden. ■

Schulungsleiter im Interview

Der erfahrene Zyxel-Kursleiter **Patrick Hirscher** beantwortet im Interview die wichtigsten Fragen zum Thema Erpressersoftware (Ransomware) und gibt nützliche Tipps aus erster Hand.

Wie beurteilen Sie die Bedrohungslage durch Erpressersoftware (Ransomware)?
Die Gefahr ist sehr groß, wachsend und noch schwer einzuschätzen. In einem Punkt ist man sich beim Thema Erpressersoftware (Ransomware) jedoch einig: Die Lösung für sämtliche Probleme in diesem Bereich gibt es leider noch nicht. Offensichtlich ist sich die IT-Industrie dessen bewusst und lässt alle hoffen. Vorerst müssen wir also mit der aktuellen Situation zurechtkommen und uns mit den zur Verfügung stehenden Lösungen möglichst schadlos halten.

Wie kann man das Bewusstsein vor Erpressersoftware (Ransomware) bei den Anwendern stärken?
Die Einschätzung der Vertrauenswürdigkeit an einem konkreten Fall ist in unserem Unternehmen zu 100 Prozent schief gelaufen. Eine sehr gut gefälschte Bewerbung wurde als E-Mail über drei Instanzen weitergeleitet. Eine Person öffnete schlussendlich die mit Erpressersoftware (Ransomware) befallene Bewerbungsdatei. Dies trotz einer Makrowarnung seitens Word. Glücklicherweise konnte der auf dem Client installierte Virenscanner Schlimmeres verhindern. Im Anschluss an diesen Vorfall führten wir intern einen für alle Mitarbeitenden obligatorischen Security-Kurs durch, in welchem wir den erwähnten Fall offenlegten und daraus lernen konnten. Ich bin davon überzeugt, dass die dafür eingesetzte Zeit einen wesentlichen Beitrag zum korrekten Umgang mit Informationen aus unterschiedlichen Quellen (Mail, Browser usw.) geschaffen hat. In Zukunft werden wir weitere interne Awareness-Schulungen durchführen.

Wie wird Erpressersoftware (Ransomware) bereits in einkommenden Mails blockiert?
Als erste Instanz wird auf jeden Fall eine Antispam-Lösung mit integriertem Virenscanner benötigt. Ransomware-Angriffe werden aber zunehmend raffinierter und leider von Spam-Lösungen trotz neuster Sandbox-Technologie oft nicht erkannt. Bei Zyxel werden alle Mails mit verdächtigen Attachments geblockt und in eine Quarantäne gestellt. Dies hat allerdings Konsequenzen: Die Quarantäne wird von einem IT-Mitarbeiter manuell bedient, der das Mail auf seine Vertrauenswürdigkeit hin überprüft und anschließend dem Adressaten freigibt. Diese Umsetzung führt zu einem großen Aufwand, ist in der aktuellen Bedrohungslage jedoch sehr wirkungsvoll. Im Weiteren werden für öffentliche Mailkonten, welche viele allgemeine und potenziell gefährliche Mails behandeln, dedizierte Arbeitsplätze eingesetzt. Der angemeldete Benutzer arbeitet mit stark eingeschränkter Berechtigung auf dem Fileserver. Bei einem Ransomware-Befall wäre der Schaden limitiert und unter Kontrolle.

Wie werden Systeme gegen Erpressersoftware (Ransomware) möglichst immun?
Ein Muss ist das Aktualisieren von Betriebssystemen und Anwendungen. In diesem Bereich setzen wir kompromisslos auf „Schnelligkeit". Sobald neue Updates von Herstellern zur Verfügung stehen, spielen wir diese so zeitnah wie möglich ein. Dies geschieht nicht mehr nur an angrenzenden Wochenenden, sondern auch im Verlauf des Tagesgeschäfts. Grundsätzlich sind wir von dieser Notwendigkeit überzeugt, kämpfen allerdings mit der Erstellung eines verlässlichen Berichts, der zeigt, dass alle Clients jeweils die aktuellste Version aufweisen.

Was ist bei der Datensicherung mit Backups zu beachten?
Oft führen bei erfolgreichen Crypto-Attacken nur noch die vorhandenen Sicherungen zu den benötigten Daten. Wir haben sichergestellt, dass nach einem erfolgten Backup die gesicherten Daten vom Unternehmens-netzwerk getrennt werden.

Welche weiteren Aktionen sind bei Zyxel geplant?
- Einsatz von FW4.20 auf Zyxel-Firewall USG1900 (mit GeoIP und SafeSearch)
- Deinstallation diverser SW-Pakete auf den Clients (nur SW zur Verfügung stellen, welche benötigt wird)
- Überarbeitung der internen IT-Richtlinien
- Anpassung der Berechtigungs-Strukturen auf dem Fileserver

Welche weiteren Tipps geben Sie IT-Verantwortlichen?
Die IT-Abteilungen können einen großen Beitrag zur Sicherstellung eines Betriebs leisten, dies mit dem Einsatz diverser Systeme, welche gut unterhalten und regelmäßig auf korrekte Funktionsweise überprüft werden. Die bekannten Schadensfälle zeigen aber auf, dass oft der Faktor Mensch Schlimmeres hätte verhindern können. Somit ist es sinnvoll, die Mitarbeitenden regelmäßig zu schulen und gezielt auf neue Gefahren hin zu informieren. Also, nehmen Sie sich die notwendige Zeit zur Schaffung einer guten Awareness, es lohnt sich!

ZYXEL

Your Networking Ally

Deutschland und Österreich
Zyxel Deutschland GmbH
Adenauerstrasse 20/B2
D-52146 Würselen

Tel.: +49 (0) 2405 – 69 09 0
Fax: +49 (0) 2405 – 69 09 510
E-Mail: sales@zyxel.de