So fallen sie Ransomware nicht zum Opfer

Was kleine, mittlere und dezentral aufgestellte Unternehmen über den ausgeklügelten Malware-Angriff wissen müssen, der Firmen plagt und weltweit Schlagzeilen macht

WatchGuard®

WAS IST RANSOMWARE?

Der Begriff Ransomware bezieht sich auf Schadprogramme, die Ihnen den Zugriff auf Ihren Computer verwehren bzw. die darauf befindlichen Informationen verschlüsseln, um dann von Ihnen ein „Lösegeld“ für die Bereitstellung des Entschlüsselungscodes bzw. die Freigabe zu fordern.

WAS BEDEUTET DAS FÜR MICH?

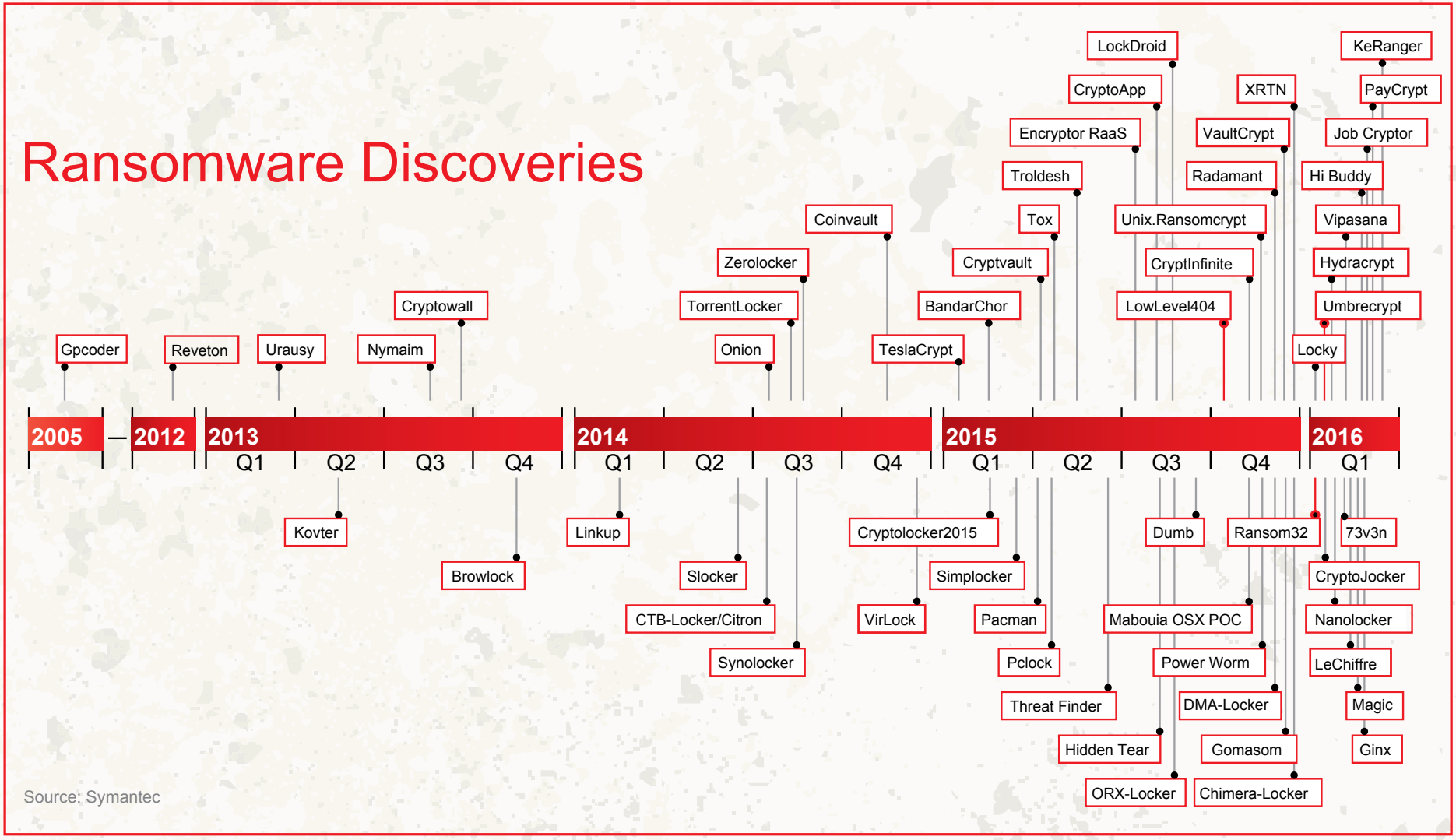
Berichte zeigen, dass 42 Prozent der kleinen und mittelständischen Unternehmen Crypto-Malware (also beispielsweise Ransomware) als eine der gefährlichsten Bedrohungen erachten, denen sie derzeit ausgesetzt sind – und das aus gutem Grund! Ransomware-Angriffe richten sich zunehmend gegen kleine und mittlere Unternehmen sowie Unternehmen mit verteilten Standorten, denn gerade in solchen Organisationen ist das Netzwerk häufig lückenhaft abgesichert, sodass perfide Malware, also auch Ransomware, nur unzureichend erkannt und abgewehrt werden kann. Internetkriminelle betrachten kleine und mittlere Unternehmen sowie Unternehmen mit verteilten Standorten häufig als „leichte Beute“! Während in der Regel um die 300 US-Dollar Lösegeld gefordert werden, zeigen Studien, dass ein einzelner Ransomware-Angriff kleine und mittlere Unternehmen durchschnittlich in Summe bis zu 99.000 US-Dollar kosten kann.

In diesem E-Book werden wir einige der wichtigsten Trends aufzeigen, die bei der Verbreitung von Ransomware zu beobachten sind, und Strategien bzw. Best Practices zur Abwehr derartiger Angriffe vorstellen.

42 Prozent der kleinen und mittleren Unternehmen betrachten Crypto-Malware als die gefährlichste Bedrohung, der sie zurzeit ausgesetzt sind.

RANSOMWARE GEWINNT AN BEDEUTUNG

Ransomware entwickelt sich in zunehmendem Maße zu einer gängigen Methode, mit der Hacker Angriffe gegen Einzelpersonen, kleine und mittlere Unternehmen sowie Unternehmen mit verteilten Standorten führen. Bereits 2005 wurden die ersten Ransomware-Vorfälle erkannt, in den letzten drei Jahren jedoch hat diese Art von Bedrohung explosionsartig zugenommen und Millionen von Computern und mobilen Geräten weltweit betroffen.



RANSOMWARE DREHT DEN SPIESS UM

Bei der Klärung von Sicherheitsfragen geht es häufig darum, sensible Daten zu schützen und Angreifern, die diese Daten für ihre eigenen Zwecke nutzen könnten, einen Riegel vorzuschieben. In öffentlichen wie auch in privaten Organisationen hat es bereits massive Sicherheitsverletzungen gegeben, die enorme finanzielle Verluste zur Folge hatten, weil Kriminelle personenbezogene Daten und Kreditkartennummern gestohlen und damit weitere Straftaten begangen haben. Die Nachwirkungen derartiger Übergriffe – beispielsweise der Imageschaden für das Unternehmen und der Vertrauensverlust bei den Kunden – sind häufig nur schwer zu quantifizieren.

Das Rezept zur Abwehr derartiger Angriffe ist bis dato weitgehend unverändert geblieben: sensible Daten identifizieren, Schutzwälle um die Speicher- und Nutzungsorte dieser Daten errichten und die Daten selbst möglichst auch verschlüsseln.

Ransomware dreht den Spieß um, denn jetzt werden Ihre Daten gekidnappt, um ein Lösegeld fordern zu können. Dabei ist der Angreifer an den Daten selbst kaum interessiert. Wichtig für ihn ist, wie wertvoll diese Daten für Sie (oder Ihre Organisation) sind. Genauer gesagt: Selbst wenn es sich nicht um sonderlich sensible Inhalte handelt, werden diese Daten möglicherweise kurz- oder langfristig dringend für die betrieblichen Abläufe in Ihrer Organisation benötigt.

KOMMERZIALISIERUNG UND RANSOMWARE-AS-A-SERVICE

Das Darknet ist ein wahres Mekka für Kriminelle, denn hier kann jeder unqualifizierte Hacker – oder auch jeder normale Bürger – alles kaufen, was man für einen heimtückischen Malware-Angriff braucht. Diese Kommerzialisierung von Malware-Anwendungen und -Werkzeugen ermöglicht es Hackern, sich bestimmte Malware-Typen für gezielte Angriffe gegen kleine und mittlere Unternehmen sowie Unternehmen mit verteilten Standorten zu beschaffen – ohne viel Zeit und Energie investieren zu müssen. Da zahlreiche dieser anvisierten Unternehmen nicht über die notwendigen Schutzeinrichtungen verfügen, werden viele von ihnen Ransomware-Angriffen zum Opfer fallen, die eigentlich hätten vermieden werden können.

Durch das Aufkommen von Ransomware-as-a-Service verschärft sich dieses Problem zusätzlich. Selbst technischen Laien mit kriminellen Ambitionen bietet Ransomware-as-a-Service die Chance, raffinierte Malware-Angriffe nicht nur durchzuführen, sondern sich außerdem die damit erpressten Erlöse zu sichern.

ZIELGERICHTETE RANSOMWARE ETABLIERT SICH

Bisher erfolgten Ransomware-Infektionen breit gestreut über Phishing-E-Mails mit bösartigen Links als so genannte „Spray-Angriffe". Hacker versenden Massen-E-Mails und versuchen, damit so viele Personen wie möglich zu infizieren. Jeden Tag werden Tausende dieser E-Mails verschickt, wobei die Angreifer lediglich auf die Masse der Empfänger setzen und hoffen, dass irgendjemand naiv genug ist, auf einen Link zu klicken oder die Datei eines Absenders herunterzuladen, den er nicht kennt. Die traurige Wahrheit ist, dass auf diese Weise zahlreiche Infektionen erfolgen. Dies wird durch den hohen Anteil der Organisationen (**85 Prozent**) belegt, die 2015 Opfer eines Phishing-Angriffs waren.

Solche breit gestreuten Angriffe sind zwar weiterhin erfolgreich, immer häufiger kommt es allerdings zu gezielten Spear-Phishing-Versuchen. Untersuchungen haben ergeben, dass **die Anzahl der Spear-Phishing-Angriffe von 2014 auf 2015 um 22 Prozent gestiegen ist**. Heutzutage nehmen erfahrene Hacker sich die Zeit, ein Ziel genauer zu untersuchen, eine überzeugende E-Mail zu verfassen (sich vielleicht sogar für einen Kollegen oder Freund auszugeben) und Malware methodisch zu gestalten, um die Erfolgsquote bei Ransomware-Angriffen zu verbessern. Bevorzugtes Ziel von Spear-Phishing-Kampagnen sind kleine und mittelständische Unternehmen: 43 Prozent entsprechender Angriffe hatten Unternehmen mit 250 oder weniger Mitarbeitern im Visier.

Hinzu kommt, dass diese Angriffe konkret auf bestimmte Ziele gerichtet sind und deshalb weitaus größeren Schaden anrichten können. Mittlerweile gibt es eine neue Ransomware-Gattung, die Sicherungskopien und Cloud-Speicher ausfindig macht, sodass es für Sie schwieriger – wenn nicht gar unmöglich – wird, Ihre Daten wiederherzustellen.
Neue Entwicklungen gibt es auch hinsichtlich der Lösegeldforderung: Die Summen richten sich nach Organisation und Umfeld des Ransomware-Opfers.

MITARBEITER SIND DAS SCHWÄCHSTE GLIED

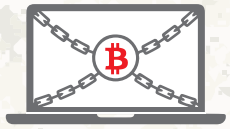
Seit langem schon nutzen Kriminelle sogenannte Social-Engineering-Methoden, um ihre Opfer gezielt zu manipulieren. Hierbei führt unter anderem Einschüchterung häufig zum Erfolg: Der Absender gibt sich beispielsweise als offizielle Behörde bzw. die Polizei aus, um Malware über sorgsam ausgearbeitete E-Mails, die an eine vorab als Opfer auserkorene Person gerichtet sind, ins Unternehmen einzuschleusen. Social Engineering spielt in diesem Zusammenhang eine entscheidende Rolle. Ihre Mitarbeiter stehen im Kampf gegen Ransomware also an vorderster Front.

Ein Klick eines arglosen Mitarbeiters in der Buchhaltung auf eine Phishing-E-Mail genügt, und schon ist das System gehackt, Geräte werden gesperrt und das Geschäft für diesen Tag ist gelaufen. Ganz gleich, ob es sich um breit gestreute oder gezielte Angriffsversuche handelt, wichtig ist, dass Ihre Mitarbeiter wissen, wie eine Phishing-E-Mail aussieht und was sie bewirken kann.

RANSOMWARE-BEDROHUNG ABWEHREN

In den letzten Jahren ist die Anzahl von Ransomware-Vorfällen explosionsartig angestiegen. Weltweit wurden hunderttausende Systeme infiziert. Der einfache Zugriff auf Ransomware-Werkzeuge und das Aufkommen von Ransomware-as-a-Service haben dazu geführt, dass Hacker heutzutage nicht mehr unbedingt versierte Technik-Freaks sein müssen. Durch die Verfügbarkeit dieser Tools hat es zwar insgesamt deutlich mehr Ransomware-Angriffe gegeben, doch können mittlerweile viele davon verhindert werden.

Die Total Security Suite von WatchGuard ist der erste UTM-Service, der kleinen und mittleren Unternehmen effektive Mechanismen zur Abwehr von Ransomware-Angriffen zur Verfügung stellt. Mit ausgereiften Sicherheitslösungen wie WebBlocker, APT Blocker und Host Ransomware Prevention ist WatchGuard Total Security die beste Wahl für jedes Unternehmen, das sich wirksam vor Ransomware-Angriffen schützen will.

WEBBLOCKER 	WebBlocker ist ein vollständig integrierter Sicherheitsdienst für WatchGuard-Appliances, mit dem IT-Administratoren Zugriffe auf Internetseiten und -inhalte gezielt steuern sowie das Surfverhalten kontrollieren können. Dieses Modul blockiert bösartige Websites, auf denen sich Ransomware eingenistet haben könnte, und verhindert so den Download von Malware.
APT BLOCKER 	APT Blocker ist eine dynamische Sandbox-Lösung, die das Verhalten von Schadprogrammen visualisiert und analysiert. Bisher unbekannte Dateien werden in einer virtuellen Umgebung aufgebrochen, um ihr Verhalten zu analysieren und das Bedrohungspotenzial zu bestimmen. Auf diese Weise schützt APT Blocker Ihre Systeme vor fortschrittlicher Malware und Zero-Day-Bedrohungen.
HOST RANSOMWARE PREVENTION 	Host Ransomware Prevention (HRP) erkennt und verhindert Ransomware-Angriffe am Endpunkt. Mithilfe von Verhaltensanalysen überprüft HRP eine Vielzahl von Merkmalen am Endpunkt und ist somit in der Lage zu erkennen, ob ein Ereignis mit einem Ransomware-Angriff in Verbindung steht oder nicht. Bei ernsthaften Gefahren kann HRP die Ausführung verhindern, noch bevor eine Dateiverschlüsselung stattfindet.

Threat Detection and Response (TDR) von WatchGuard bietet kleinen, mittelständischen und dezentral aufgestellten Unternehmen Korrelationsfunktionen auf Enterprise-Niveau. Wann immer Sie ein Problem vermuten: Branchenführende Lösungen beleuchten Ihren Endpunkt, erkennen und korrelieren Bedrohungen und schützen Ihre wichtigsten Vermögenswerte.

WatchGuard® Technologies gehört zu den weltweit führenden Anbietern von integrierten multifunktionalen Sicherheitslösungen im Unternehmensumfeld. Das Erfolgsrezept beruht auf der ausgeklügelten Kombination von leistungsstarker Hardware, fortschrittlicher Sicherheitsfunktionalität und effektiven, Policy-basierten Verwaltungsmöglichkeiten. Damit bietet WatchGuard Hunderttausenden von Unternehmen weltweit einfach zu bedienende Sicherheitsprodukte auf Enterprise-Niveau. Weitere Informationen finden Sie unter **WatchGuard.com/TDR**.