CRYPTOTROJANER/ RANSOMWARE*

Die häufigsten Fehler & wichtige Sofortmaßnahmen

Ihre Datensicherheit auf dem Prüfstand

Von Kreditkarteninformationen bis hin zu den Profilen unserer Kinder: Das Thema Datensicherheit wird derzeit im Wochentakt vor ganz neue Herausforderungen gestellt.

Ransomware wie LOCKY, eingeschmuggelt per USB Stick oder eMail, nimmt immer häufiger ganze Infrastrukturen als Geisel.

Aktuelle Meldungen betreffen Unternehmen und Institutionen von Krankenhäusern bis hin zu infizierten Regierungseinrichtungen.

Die mediale Aufmerksamkeit, die z.B. LOCKY aktuell erhält, spornt die Entwickler zu einer ganz neuen Dynamik in der Weiterentwicklung an. Beinahe wöchentlich tauchen aktualisierte Versionen auf, hinzu kommen Trittbrettfahrer welche versuchen die „gut funktionierenden" Schwachstellen ebenfalls auszunutzen.

DIE 3 HÄUFIGSTEN FEHLER IN DER PRÄVENTION

1

„DER VIRENSCANNER WIRD'S SCHON RICHTEN."

Erst seit Kurzem bieten einige der Premiumanbieter überhaupt einen Schutz in diesem Bereich an. Daher ist der Virenscanner nur als (sinnvolle!) Ergänzung anzusehen. Ein umfassender Schutz muss wesentlich ganzheitlicher angegangen werden.

2

„MEINE MITARBEITER SIND DOCH NICHT BLÖD."

Natürlich sind sie das nicht!
Das Thema IT-Sicherheit betrifft dank der jüngsten Entwicklungen jedoch JEDEN Mitarbeiter mit Zugang zu Ihrem Netzwerk, vom Azubi über die Buchhaltung bis zum Vertrieb. Der eigentliche Gefahrenfaktor heißt daher „Unwissenheit".

3

„WIR HABEN BACKUPS, ALLES IST GUT."

Unter anderem die Art und Weise Ihrer Backups entscheidet. Von Natur aus ist Ransomware genau darauf ausgelegt in diesem Bereich z.B. nach angeschlossenen Laufwerken zu suchen für eine effiziente „Geiselnahme". Einmal verschlüsselt sind auch betroffene Backups dauerhaft unbrauchbar.

?

Who the F*ck is LOCKY?

Anders als der ähnlich klingende Loki, seines Zeichens Gott der Lügen und Streiche, bekannt aus der Mythologie (oder Marvel's Avengers), ist LOCKY, ebenso wie seine „Kollegen" CRYPTOWALL, TESLACRYPT u.a., eine von Menschen geschaffene und durchaus realistische Bedrohung.
Vor allem über Schwachstellen in Microsoft Office und Javascript installiert sich die Schadsoftware unbemerkt und nimmt dann spektakulär ganze Systeme in „Geiselhaft". Mehr zum Thema Ransomware finden Sie im Infokasten am Ende von Seite 2.

WICHTIG UND RICHTIG:
Gehen Sie offen mit der Gefahr um!

Vorbei sind die Zeiten in denen man sich Trojaner & Co. nur auf „einschlägigen, schmuddeligen" oder illegalen Seiten „eingefangen" hat und man eine Infektion demnach lieber im stillen Kämmerlein gelöst hat.

Woher kommt die momentane Infektionswelle mit Ransomware?

Obwohl in den meisten Unternehmen moderne Sicherheitsmechanismen (Firewalls, Virenscanner, Anti-Spam-Gateways, uvm.) selbstverständlich sind, treten aktuell weltweit eine große Anzahl von Infektionen mit Verschlüsselungstrojanern auf.

Eine typische Infektion kann dabei wie folgt ablaufen:
Sie erhalten eine E-Mail, die von einem plausiblen Absender zu stammen scheint, z.B. einem Kollegen, einem Netzwerkscanner, einem Paketdienst oder einem externen Unternehmen.

Diese E-Mail enthält als Anhang eine Word oder Excel-Datei mit einem eingebetteten Makro (getarnt als Rechnung, gescanntes Dokument o.ä.). Wenn der Empfänger das Dokument öffnet, startet dieses Makro das Herunterladen der eigentlichen Schadsoftware von einer Reihe nur für kurze Zeit existierender Internetadressen. Geschicktes Social Engineering bereits in der Email („Sollte die Codierung des angehängten Dokuments fehlerhaft erscheint, aktivieren Sie bitte die Ausführung von Makros. Das geht wie folgt…") trickst auch Nutzer von Installationen mit manueller Bestätigung aus. Nach dem Download führt das Makro den Cryptotrojaner aus und lädt einen für diesen speziellen Rechner individuell erstellten Schlüssel herunter.

Mit diesem werden dann Dateien und Ordner auf dem Rechner sowie auf den erreichbaren Netzlaufwerken verschlüsselt. Sicherheitskopien des Windows-Betriebssystems werden häufig gelöscht oder ebenfalls verschlüsselt, nun wird dem Benutzer eine Nachricht dargestellt, wie ein Lösegeld gezahlt werden kann, um ein passendes Entschlüsselungstool zu erhalten.
Bitte beachten Sie: Dies ist nur ein einziges Beispiel, wie eine solche Infektion ablaufen kann. Andere Schädlinge nutzen teilweise andere/weitere Infektionswege, Verschlüsselungsverfahren und Kommunikationswege.

*Was ist ein Cryptotrojaner/ Ransomware?

Es handelt sich hier um Schadsoftware, die auf den verschiedensten Wegen (via eMail, Downloads, Browserlücken oder „Fremd"-USB Sticks) zu Ihnen finden kann.
Durch einen Verschlüsselungsalgorithmus werden dann Ihre Daten und Laufwerke so eingekapselt, dass Sie diese nicht mehr öffnen können.
Üblicherweise werden Sie nach Abschluss der Verschlüsselung dazu aufgefordert eine gewisse Summe zu bezahlen, damit die Daten wieder entschlüsselt werden. Ohne dieses „Lösegeld" von üblicherweise 400-500$ bleiben Ihre Daten unbrauchbar.

Warum sind diese Trojaner so erfolgreich?

Die Entwickler der Schadsoftware haben den Markt sehr genau analysiert und machen sich die am häufigsten vorkommenden Schwachstellen und falsch gesetzten unternehmerischen Prioritäten gezielt zu Nutze:

- Nicht ausreichende Schulung der Benutzer („Welche Dokumente (und von wem) darf ich öffnen?", "Was, wenn ein vom Typ eigentlich gesperrtes Dokument empfangen werden muss?", „Wie erkenne ich eine Phishing-Email?")
- Mangelhaftes Benutzer-/Rechtekonzept (Benutzer arbeiten als Administratoren und haben z.B. pauschal mehr Rechte auf Netzlaufwerken, als für ihre Aufgabe notwendig ist)
- Rudimentäres Backupkonzept (Backups nicht zeitnah, nicht offline/ offsite). Updates/Patches für Betriebssystem und Anwendungen werden nicht zeitnah eingespielt
- Unwissenheit der Admins im Bereich der IT-Sicherheit (z.B. häufig: .exe-Dateien werden in E-Mails blockiert, nicht aber Office-Makros oder andere aktive Inhalte)
- Fehler in der Konfiguration der Systeme und der Netzwerksegmentierung (Server und Workstations im gleichen Netz).

Das häufig kombinierte Auftreten aus Unwissenheit und - meist aus personellen oder organisatorischen Gründen („Wir wissen, dass das nicht sicher ist, aber die Leute müssen doch arbeiten…") - lückenhaften Prozessen und Konfigurationen begünstigt die schnelle Verbreitung auch auf z.B. Ihre Geschäftspartner sobald ein solcher Trojaner einmal aktiviert wurde.

WICHTIG UND RICHTIG:
Lassen Sie Profis helfen

Es ist **kein** Zeichen von Unsicherheit oder gar Inkompetenz, sich helfen zu lassen. Im Gegenteil: Sie haben das Ausmaß der Bedrohung richtig erkannt und handeln im Sinne Ihres Unternehmens!

DER NETTE GEISELNEHMER VON NEBENAN?

So ärgerlich und bedrohlich ein verschlüsseltes System auch ist: Bisher waren die Hersteller der Trojaner meist „recht nett". Denn häufig liefern die Online-Erpresser gegen die Bezahlung des Lösegelds (bisher) tatsächlich das Entschlüsselungstool aus . So gesehen bei z.B. einem Unternehmen in Grafschaft (Rheinland-Pfalz). **Grundsätzlich ist von der Zahlung eines Lösegelds jedoch abzuraten,** da eine solch effiziente und ertragreiche Verdienstmöglichkeit entsprechend schnell an weiterer Popularität gewinnt.
Meldungen über Trittbrettfahrer und Fälle von gezahltem Geld **ohne** anschliessender Auslieferung eines Dechiffrierschlüssels werden immer häufiger. **Das BSI rät ebenfalls, kein Lösegeld zu zahlen und in jedem Fall Anzeige zu erstatten.**
Prävention ist hier Ihre mächtigste Waffe: Nicht nur Technologie, sondern in mindestens gleichem Maße auch die Kompetenz Ihrer Mitarbeiter ist hier gefragt. Auf der nächsten Seite finden Sie die wichtigsten Sofort- und weiterführenden Maßnahmen zum Schutz Ihres Unternehmens ohne Ihre Mitarbeiter zu frustrieren oder Projekte zu behindern.

WICHTIG UND RICHTIG:
Selbstehrlichkeit

Viele Maßnahmen können bereits mit Bordmitteln oder vorhandener Ausstattung aufgesetzt werden. Dafür und für alles andere müssen Sie heute kein Experte sein - LastBreach hat diese oder macht Sie auch gerne selbst zu einem!

Sofortmaßnahmen

Die schlechte Nachricht vorab: Wie Sie wahrscheinlich bereits vermuten: eine 100%-ige Sicherheit gibt es tatsächlich nicht. Die Gute: Sie können das Risiko und die Auswirkungen tatsächlich sehr effektiv minimieren.

Backups offline/offsite

Definieren Sie eine Wiederherstellungsstrategie (System-/ Daten-Rollback, Neuinstallation) Sorgen Sie für regelmäßige Backups. Das einfache Kopieren in ein anderes Laufwerk ist hierbei jedoch nicht der richtige Weg, da Cryptotrojaner auch angebundene Laufwerke befallen. Eine Alternative bzw. Ergänzung zu Backups kann eine private Cloud mit Historisierung und Rollback sein, sodass bei Befall die „alten" Daten wieder zurückgeholt werden können.
Berücksichtigen Sie, dass nicht nur der Ausfall einer Hardware abgesichert ist, sondern auch der Online-Zugriff auf Sicherungen z.B. durch Trojaner auf Admin-Rechnern nicht möglich ist.
Backups sollten zudem auch Offsite, also. örtlich getrennt, aufbewahrt werden.

Patches und Updates einspielen

Veraltete Anwendungen und Betriebssysteme sind der primäre Weg, über den Systeme mit Schadsoftware infiziert werden. Ein zentrales Update- und Patchmanagement sorgt hier für das zeitnahe Einspielen der Updates und Patches. Dies darf nicht dem Endnutzer überlassen werden, welchem im Regelfalle das Verständnis und Know-How dafür fehlt.

Admin- und weitere Zugriffsrechte verwalten

Jeder Benutzer sollte immer nur mit den Rechten ausgestattet sein, die zur Erfüllung seiner Aufgabe notwendig sind. Es gibt nur sehr wenige Gründe, warum ein Mitarbeiter beim Arbeiten mit seinen Geschäftsanwendungen als Administrator angemeldet sein müsste oder warum er auf Netzlaufwerke zugreifen darf, die er nicht (mehr) zur Erfüllung seiner Aufgaben benötigt.

Generelle Prioritäten setzen (Beispiel: MS Office-Makros)

In einer ActiveDirectory Umgebung können Makros per Gruppenrichtlinie zentral deaktiviert werden. Für die Mitarbeiter, die aufgrund ihrer Tätigkeit diese Funktionalität benötigen, kann diese Funktion ebenso zentral freigeschaltet werden.

Virenschutz, Email- und Web-Gateways, Firewalls, etc. richtig konfigurieren

Dieser Bereich ist natürlich hochgradig spezifisch im Bezug auf Ihre eigene Umgebung, daher können wir wenig pauschale Empfehlungen machen. Generell ist hier jedoch zu prüfen ob z.B. Ihr Email-Gateway Sandboxing unterstützt und Quarantäneregeln lückenlos eingerichtet sind; ob Ihr Web-Gateway wirksam die Kommunikation mit den Command & Control-Servern der Trojaner unterbindet und der Virenschutz bestmöglich konfiguriert und verteilt ist.

Weiterführende Maßnahmen

Schulen Sie alle Ihre Mitarbeiter

Die bisherigen Sofortmaßnahmen betreffen die Mitarbeiter, die sowieso tagtäglich auf Systemebene mit Ihrem Netzwerk umgehen. Die besten Technologien und Maßnahmen versagen jedoch, wenn der Azubi nicht wusste, dass nur freigegebene USB-Sticks im Unternehmen genutzt werden dürfen. Regelmäßige, transparente und für den „Nicht-IT'ler" verständliche Schulungen sind also notwendig damit das gesamte Team hier dieselbe Sprache spricht.
Sicherheitsmaßnahmen dürfen nicht als Gängelung oder Behinderung der täglichen Arbeit wahrgenommen werden, sondern müssen ein Selbstverständnis für das Wohl des Unternehmens, der Mitarbeiter und aller Kunden sein.

Behandeln Sie Security als ganzheitliches Konzept

Technisch können Sie von der Segmentierung Ihres Firmennetzwerks über die Nutzung von Security-Analysetools bis hin zum Mobile Management unglaublich viele Maßnahmen ergreifen. Diese bieten jedoch keinen umfassenden Schutz wenn sie nicht aufeinander abgestimmt sind und Best Practices nicht umgesetzt werden (siehe oben: die Themen Unwissenheit und Security als Störung). Meist ist es am effizientesten wenn man die eigenen Stärken und Schwächen analysiert und dann entsprechend Experten konsultiert.

Sie ahnen es vermutlich bereits: Wir bei LastBreach haben uns darauf spezialisiert, Unternehmen zu helfen die IT-Sicherheit auf bestmöglichem Niveau zu betreiben **ohne** dabei die Mitarbeitermoral oder Projekte negativ zu beeinflussen.

DIREKTKONTAKT

Frederic Mohr
Security Consultant
fredericmohr@lastbreach.com
Tel.:+49 (0) 89 3078 4343

Max Körbächer
Security Consultant
maxkoerbaecher@lastbreach.com
Tel.:+49 (0) 89 3078 4343

Tobias Kirchherr
Sales/ Marketing
tobiaskirchherr@lastbreach.com
Tel.:+49 (0) 171 8192079

Testen Sie uns jetzt und reagieren Sie professionell, schnell und effizient auf die aktuellsten Bedrohungen aus dem Internet!

KEEP CALM AND...

Dieses Whitepaper soll Sie nicht dazu veranlassen, nun mit den Händen über dem Kopf, wild schreiend, alles und jeden zu überprüfen. Bleiben Sie ruhig, überlegen Sie sich in welchen Bereichen Sie wissen dass es bereits ausreichende Maßnahmen gibt und in welchen nicht. **LastBreach** bietet Ihnen ein **kostenloses und unverbindliches Security-Assessment** an in welchem Sie einen Einblick in die aktuelle Arbeitsweise der Hacking Community im Abgleich mit Ihren aktuellen Maßnahmen erhalten.

Über LastBreach

LastBreach ist eine IT-Sicherheitsfirma die 2015 in München gegründet wurde und bestrebt ist, IT-Sicherheit zu liefern die Ihre Assets absichert und Ihr Geschäft unterstützt.

IT-Sicherheit hat bedauerlicherweise den schlechten Ruf dem Unternehmen in die Quere zu kommen. Projekte können nicht starten da sie nicht die Sicherheitsbestimmungen erfüllen, Mitarbeiter fühlen sich dazu berufen Alternativen zu finden um die Security Policies zu umgehen, das Budget für Sicherheit scheint in einem bodenlosem Fass zu verschwinden und die IT-Abteilung kämpft sich durch all diese Umstände.

Wir haben es uns zur Aufgabe gemacht, maßgeschneiderte Sicherheitsdienstleistungen an unsere Kunden zu liefern, welche auf der einen Seite wichtige Assets schützen, auf der anderen Seite aber auch die Mitarbeitermoral nicht negativ beeinflussen und Projekte am laufen halten. Zu diesem Zweck erhalten all unsere Mitarbeiter regelmäßig Schulungen in IT-Sicherheit. Dies erlaubt es uns, aus den unterschiedlichsten Blickwinkeln ein Unternehmen zu betrachten und so Probleme frühzeitig zu identifizieren die in der Regel nicht ersichtlich wären. Wir nutzen die Synergie zwischen der Technologie, dem Management und den Mitarbeitern um eine passende Lösung zu finden, die keine negativen Auswirkungen auf die tägliche Arbeit haben.

Wir engagieren uns außerdem in der IT-Security Community und arbeiten mit Open-Source Projekten zusammen um die Weiterentwicklung kostenfreier IT-Lösungen zu unterstützen. Sie finden uns auf Konferenzen, lokalen IT-Treffen und natürlich auch in den sozialen Netzen wie XING, LinkedIn, Twitter, Youtube, Google+ und Facebook.

LastBreach UG (haftungsbeschränkt)
Rohrauerstr. 69
81477 München
Telefon: +49 (0) 89 3078 4343
Telefax: +49 (0) 89 20002108
E-Mail: fredericmohr@lastbreach.com
Internet: http://lastbreach.com