Link: https://www.cio.de/a/schutz-vor-cyber-erpressern,3229580

Webcast

Schutz vor Cyber-Erpressern

Datum: 20.06.2016
Autor(en): Christiane Pütter

Im Betreff steht „eilige Rechnung“ oder auch „Bewerbung“ – und entgegen aller Firmenrichtlinien klickt der Sachbearbeiter auf den Anhang. Den Schutz vor Cyber-Erpressern und Cryptolockern thematisiert ein Webcast der Computerwoche.

Lösegeld zahlen, um den Cyber-Erpresser wieder loszuwerden? Es gibt bessere Möglichkeiten.
Foto: Nicescene - shutterstock.com

Die größte Schwachstelle in Sicherheitsfragen bleibt der Mensch. Cyber-Kriminelle nutzen das und triggern Endanwender mit Buzzwords wie "eilige Rechnung" oder "Mahnung". Klickt das Opfer auf den entsprechenden E-Mail-Anhang, aktivieren sich schädliche Makros. Wie sich Firmen schützen können, ist Thema eines **Webcasts der Computerwoche** [1].

Christian Funk, Leiter des deutschen Forschungs- und Analyse-Teams bei Kaspersky Lab, erklärt, wie Ransomware funktioniert. Massen-Infektionen kamen 2004 auf und seitdem "professionalisieren" sich Cyber-Kriminelle ständig weiter. "Das Opfer kann heute über Bitcoin bezahlen", erklärt Funk, "die Kriminellen nehmen den User quasi an die Hand und bieten Schritt-für-Schritt-Anleitungen zum Bezahlen." Sie feilen sozusagen an der Nutzerfreundlichkeit, ironisch gesagt.

Dem Forscher ist ein gefährlicher Trend aufgefallen: Cyber-Kriminelle schreiben jetzt gerne auch "Bewerbung" in die Betreffzeile, um Aufmerksamkeit zu wecken. Und: die Erpresser entwickeln unterschiedliche Templates für unterschiedliche Länder. Sie passen Sprache und etwa die jeweilige Behörde an das Land an, Beispiel für die Bundesrepublik ist der "BKA-Trojaner". Stichwort BRD: im vergangenen Jahr ist die Zahl der Angriffe auf Deutschland um ein gutes Drittel gestiegen.

Wer nicht zahlen kann, "darf" die Ransomware weiterverbreiten

Funk nennt ein besonders perfides Beispiel: Erpresser wandten sich an eine soziale Einrichtung. Deren Entscheider antworteten, sie hätten das Geld einfach nicht, bräuchten aber ihre Daten, um arbeiten zu können. Daraufhin unterbreiteten die Kriminellen das "Angebot", die "Schulden abzuarbeiten". Was sie damit meinten? Die Einrichtung sollte die Ransomware weiterverbreiten. Moderator Korus schüttelt mit dem Kopf: "Das sind die Methoden des organisierten Verbrechens", sagt er.

Mittlerweile gibt es sogar "Ransomware-as-a-Service", berichtet Funk weiter. Das heißt: "Einer schreibt nur. Er kassiert 30 Prozent. Der Verbreiter bekommt 70 Prozent!" Er empfiehlt Betroffenen, auf jeden Fall die Polizei einzuschalten. "Natürlich herrscht erstmal Frust und die Haltung: ‚Dadurch kriege ich meine Daten auch nicht wieder', aber die Behörden sollten informiert sein", sagt Funk.

Grundsätzlich unterscheidet Kaspersky Lab zwei Subkategorien: Blocker und Verschlüsseler. Werden Dateien geblockt, ist das für das betroffene Unternehmen zwar ärgerlich, aber die Daten bleiben wenigstens erhalten. "Dann wird eben der Rechner neu aufgesetzt", sagt Funk. Anders bei Ransomware: Hier liegt der Schlüssel auf den Servern der Erpresser. "Das ist nicht ganz trivial zu Programmieren", weiß Funk. Das Aufkommen solcher Schad-Software zeigt, wie Kriminelle auf technologischer Seite "dazulernen".

Back-Up-Medien nicht permanent an den Rechner anschließen

Haupteinfallstor bleibt die E-Mail. In Sachen Prävention rät Funk zu den Klassikern: Updates durchführen und eine AV-Lösung mit einem Modul einsetzen, das Cryptor-Malware anhand des Verhaltens erkennt. Funk nennt einen oft gemachten Fehler: Das Backup-Medium ist permanent an den Rechner angeschlossen. "Man darf es bitte wirklich nur für Back-Ups verwenden", so sein Appell. Das gilt nicht nur für Unternehmen, sondern auch für Privatanwender.

Moderator Korus will von den Webcast-Zuschauern wissen, für wie sie Ransomware einschätzen. Fazit: 31 Prozent halten sie für "extrem gefährlich", weitere 63 Prozent für "gefährlich". Funk kommentiert die gestiegene Aufmerksamkeit positiv. Er räumt aber auch ein: "Hundertprozentige Sicherheit gibt es nicht."

Das Thema wird Unternehmen künftig nicht weniger beschäftigen, erwartet der Forscher. Denn: "Es funktioniert leider zu gut." Ransomware auf Linux-Basis sei seltener - noch - aber auch "diese Kuh wird gemolken werden."

Hier den Webcast ansehen

Links im Artikel:

[1] **https://event.onlineseminarsolutions.com/eventRegistration/EventLobbyServlet?target=registration.jsp&eventid=1195956&sessionid=1&key=C918B2450DCED87646E671BE24970889&partnerref=&sourcepage=register**

IDG Tech Media GmbH
Alle Rechte vorbehalten. Jegliche Vervielfältigung oder Weiterverbreitung in jedem Medium in Teilen oder als Ganzes bedarf der schriftlichen Zustimmung der IDG Tech Media GmbH. dpa-Texte und Bilder sind urheberrechtlich geschützt und dürfen weder reproduziert noch wiederverwendet oder für gewerbliche Zwecke verwendet werden. Für den Fall, dass auf dieser Webseite unzutreffende Informationen veröffentlicht oder in Programmen oder Datenbanken Fehler enthalten sein sollten, kommt eine Haftung nur bei grober Fahrlässigkeit des Verlages oder seiner Mitarbeiter in Betracht. Die Redaktion übernimmt keine Haftung für unverlangt eingesandte Manuskripte, Fotos und Illustrationen. Für Inhalte externer Seiten, auf die von dieser Webseite aus gelinkt wird, übernimmt die IDG Tech Media GmbH keine Verantwortung.