Wenn der Erpresser zweimal klingelt

Internationale Studie von Sophos zeigt:
Jedes zweite Unternehmen war 2017 von Ransomware betroffen – im Durschnitt sogar jeweils zweimal. Hauptziel waren Unternehmen aus dem Gesundheitswesen, Deutschland liegt in „Ransomware-Ranking“ auf Platz 6.

Wiesbaden, 8. Februar 2018 – Wie stand es 2017 um die modernen IT-Gefahren für Unternehmen und wie haben sich Firmen gegen diese aufgestellt? Eine von Sophos beauftragte Befragung unter 2.700 IT-Entscheidern mittlerer Unternehmensgröße in zehn Ländern identifiziert Ransomware als eine der Hauptbedrohungen für die IT-Sicherheit: 54 Prozent aller befragten Unternehmen sahen sich 2017 Attacken durch die Erpressungssoftware ausgesetzt – und dies im Durchschnitt sogar zweifach. Der durschnittliche Schaden für Unternehmen belief sich dabei auf gut 107.000 Euro. Am meisten betroffen waren Unternehmen aus der Gesundheitsbranche, das Land mit den meisten Ransomware-Attacken war Indien. Gut 30 Prozent erwarten Ransomware-Angriffe für die Zukunft.

Befragt wurden IT-Entscheider aus den USA, Kanada, Mexiko, Frankreich, Deutschland und dem Vereinigten Königreich sowie aus Australien, Japan, Indien und Süd Afrika.

Die wichtigsten Ergebnisse auf einen Blick:

- Ransomware ist eine Schlüsselbedrohung: 54 Prozent der befragten Unternehmen wurden 2017 Opfer von Ransomware. Im Durchschnitt sogar zweimal.
- Angriffsziel Nummer eins war das Gesundheitswesen, gefolgt von Energieunternehmen und Fachdienstleistern.
- Selbst Enpoint-Secutity-Lösungen der neusten Generation sind kein hinreichender Schutz gegen Ransomware: 77 Prozent der betroffenen Unternehmen hatten zum Zeitpunkt der Attacke eine aktuelle Endpoint-Security-Lösung installiert.
- 54 Prozent der Angegriffenen hatte keine spezielle Anti-Ransomware-Lösung im Einsatz.
- Beinahe 70 Prozent der IT-Entscheider können keine Anti-Exploit-Technologien benennen.
- Nur 25 Prozent der befragten Unternehmen nutzen bereits prädiktive Sicherheitstechnologien. 68 Prozent planen für 2018 die Implementierung solcher Deep-Learning-Technologien zum Schutz gegen Ransomware und Co.

Rund 107.000 Euro Schaden für die Unternehmen

Ransomware ist eine Schlüsselbedrohung für die Unternehmenssicherheit: Indien weist dabei mit 67 Prozent den höchsten Infektionsgrad auf. Es folgen Mexiko (65 Prozent) und die USA (60 Prozent). Deutschland rangiert auf Platz 6 mit 51 Prozent. Japan bildet das Schlusslicht mit 41 Prozent.

Unternehmen zahlten einen hohen Preis für die Ransomware-Angriffe: im Durchschnitt beliefen sich die Schadenskosten auf rund 107.000 Euro. Der genaue Blick auf Deutschland zeigt, dass 63 Prozent einen Schaden zwischen 11.200 und 282.000 Euro erlitten. Die meisten, nämlich 26 Prozent, bezifferten ihre Kosten auf zwischen 56.000 und 112.000 Euro. Bemerkenswert: Im Gegensatz zu Frankreich und dem Vereinigten Königreich, wo auch Beträge im vierstelligen Bereich anfielen, kam in Deutschland kein Unternehmen mit einem Geldwert unter 11.200 Euro davon.

76 Prozent und damit die meisten Attacken hatten Unternehmen der Gesundheitsbranche im Visier. Mehr noch als Finanzdienstleister. „Ein Erklärungsansatz hierfür könnte sein, dass die Healthcare-Branche oft über eine veraltete IT-Sicherheitsinfrastruktur verfügt und somit als so genanntes Soft Target stärker von Ransomware anvisiert wird," sagt Michael Veit, Technology Evangelist bei Sophos. „Zudem kann man aufgrund der besonderen Sensibilität der Daten im Gesundheitswesen davon ausgehen, dass die Bereitschaft zu zahlen eher vorhanden ist."

Ransomware schlägt mehrfach zu

Auffallend ist die Tatsache, dass die Unternehmen in der Regel zweimal attackiert werden. Und das, obwohl die Mehrheit über ein gängiges IT-Sicherheitskonzept verfügt. Dan Schiappa, Senior Vize-Präsident und Produktmanager bei Sophos wundert das nicht: „Ransomware schlägt nicht einmal ein, sondern kann Unternehmen mehrfach treffen. Wir wissen, dass Cyberkriminelle mitunter innerhalb von einer halben Stunde bis zu vier verschiedene Ransomware-Familien freisetzen, damit mindestens eine Attacke erfolgreich ist. Wenn es den IT-Administratoren in Unternehmen nach einem Angriff außerdem nicht vollständig gelingt, die Systeme von der Schadware zu befreien, ist eine Neu-Infektion jederzeit möglich."

Was ist denn eigentlich Deep Learning?

Ein weiterer Faktor hierfür könnte an folgendem Aspekt festzumachen sein: Obwohl 60 Prozent der befragten IT-Entscheider sich darüber bewusst waren, dass ihre herkömmlichen Sicherheitskonzepte nicht mehr in genügendem Maße greifen, konnte nur ein Drittel spezielle Anti-Expoit-Technologien zum Schutz gegen moderne Cyberattacken benennen. Die Verwirrung scheint hier groß.

Dementsprechend nutzen auch nur 25 Prozent der Befragten prädiktive Next-Generation-Technologien wie Machine Learning oder Deep Learning, wie sie etwa auch die aktuelle Version von Sophos Intercept X bietet. Die Malware-Erkennung dieser Next-Gen-Endpoint Security basiert neben einer neuen Active-Hacker-Abwehr, einem fortschrittlichen Anwendungs-Lockdown und erweitertem Ransomware-Schutz auf den neuronalen Netzen des Advanced Deep Learning.

Deep Learning ist die jüngste Weiterentwicklung des Machine Learning mit einem hoch skalierbaren Erkennungsmodell, das die gesamte erkennbare Bedrohungslandschaft erlernen kann. Weil dabei Milliarden von Stichproben verarbeitet werden können, sind mit Deep

Learning im Vergleich zum herkömmlichen Machine Learning noch einmal genauere Vorhersagen möglich.

Immerhin wurde das Potential dieser Sicherheitsmodule weltweit erkannt: 68 Prozent der befragten Unternehmen planen die Implementierung in diesem Jahr. Mexiko zeigt sich mit 72 Prozent hierbei am ambitioniertesten. Auf Platz zwei folgt Deutschland mit 68 Prozent.

Alle Infos zu Deep Learning und Intercept X unter www.sophos.de/interceptx.

Bildmaterial zur Meldung finden Sie hier:
https://1drv.ms/f/s!AjxO83caq22Wm2tZ3rnT59y66woh

Über Sophos

Mehr als 100 Millionen Anwender in 150 Ländern verlassen sich auf Sophos' Complete-Security-Lösungen als den besten Schutz vor komplexen IT-Bedrohungen und Datenverlust. Sophos bietet dafür preisgekrönte Verschlüsselungs-, Endpoint-Security-, Web-, Email-, Mobile- und Network Security-Lösungen an, die einfach zu verwalten, zu installieren und einzusetzen sind. Das Angebot wird von einem weltweiten Netzwerk eigener Analysezentren, den SophosLabs, unterstützt.

Sophos hat seinen Hauptsitz in Boston, USA, und Oxford, Großbritannien. In Deutschland hat das Unternehmen seinen Hauptsitz in Wiesbaden und ist in Österreich und der Schweiz je an einem Standort vertreten. Weitere Informationen unter www.sophos.de.

Pressekontakt:

Sophos
Jörg Schindler, PR Manager CEEMEA
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de