Ransomware: Reporten oder nicht?

Ist es sinnvoll für ein Unternehmen, einen Cyberangriff bei der Polizei anzuzeigen? Experten sagen: ja!

Wiesbaden, 8. November 2016 – Opfer von Ransomware haben viel zu tun. Nachdem sie den Schock eines Angriffs und des damit verbundenen Datenverlusts durch die Verschlüsselung verkraftet haben, müssen Entscheidungen getroffen werden. Soll das Lösegeld bezahlt werden? Können alle Daten notfalls auch ohne Zahlung wiederhergestellt werden? Wie konnte es überhaupt dazu kommen? Besteht die Gefahr weiterhin und wie können wir ihr künftig begegnen? Welche Security-Tools fehlen, oder mangelt es den Mitarbeitern an Sicherheitsbewusstsein? Helfen Trainings? Erst viel weiter unten auf der langen To-Do-Liste findet sich dann: soll die Polizei eingeschaltet werden? Was haben wir davon?

Ransomware neu überdenken
„Die Reaktion auf Ransomware muss neu überdacht werden“, rät Sascha Pfeiffer, Sicherheitsexperte bei Sophos. „Das Anzeigen klassischer Straftaten wie Einbruch oder Diebstahl ist für Unternehmen selbstverständlich. Aber Online-Betrug oder Erpressung via Ransomware? Sind Computer involviert, haben betroffene Privatpersonen ebenso wie Unternehmen die Tendenz, die Straftat als das Problem des Opfers, bestenfalls noch als das der Bank oder des Providers abzutun. Das ist langfristig völlig kontraproduktiv und spielt nur den Tätern in die Hände.“

Das BSI (Bundesamt für Sicherheit in der Informationstechnologie) berichtet, dass Angriffe über Spam-E-Mails mit Anhängen, die mit Ransomware in Verbindung stehen, in Deutschland zwischen Januar und Mai 2016 um den Faktor 70 angestiegen sind. Bei 70 Prozent der betroffenen Unternehmen waren einzelne Arbeitsplatzrechner befallen. Jedes fünfte Unternehmen (22 Prozent) berichtete von einem erheblichen Ausfall von Teilen der IT-Infrastruktur und 11 Prozent erlitten einen dauerhaften Verlust wichtiger Daten. 2 Prozent der Betroffenen gaben an, dass durch die Ransomware-Infektion die wirtschaftliche Existenz des Unternehmens bedroht ist oder war.

Angesichts der zunehmenden Online-Kriminalität, haben Polizei und Regierung schon länger erkannt, dass dieser nur sinnvoll begegnet werden kann, wenn man sie wie jede andere Straftat auch behandelt. Intelligenz ist notwendig, um die Öffentlichkeit von Anschlägen zu warnen, Beweise für Anklagen zusammenzutragen und Täter zu überführen.

Hierzu müssen Betroffene allerdings mit dem gewohnten Schweigen brechen und anfangen, mit den Strafverfolgungsbehörden zusammenzuarbeiten. Ihre Untersuchungen sind immens wichtig. Ohne Echtzeitberichterstattung ist es unmöglich zu wissen, welche Ziele die Kriminellen aktuell verfolgen und vorhandene Beweismittel zu sichern.

Soll man Ransomware melden?
Unbedingt. Ohne eine sorgfältige Prüfung der Geschehnisse und Sicherstellung der Beweismittel ist eine Ermittlung der Geschehnisse und der Täter ausgeschlossen. Langfristig ist das kein Szenario, das den Unternehmen, der Geschäftswelt und der Öffentlichkeit dient. Profitieren würden nur die Angreifer.

Erst vor wenigen Wochen veröffentlichte das FBI eine Informationsschrift in der sie die Opfer von Ransomware ermunterte, Angriffe dem „Agencies Crime Complaint Center (IC3)“ detailliert zu melden.Aber auch in Europa ist man nicht untätig. Ein paar Monate zuvor startete Europol, die niederländische Polizei und eine Gruppe von Cybersicherheitsfirmen die Initiative „No More Ransom“. Sie bietet Betroffenen einen ersten Anlaufpunkt für Fragen, etwa dazu, ob Anzeige erstattet werden soll und was als nächstes zu tun ist.

In Großbritannien können Ransomware- und Phishing-Angriffe bereits über ein Online-Tool gemeldet werden und das britische Büro für nationale Statistiken (ONS) widmete der neuen Kriminalitätsform in seiner 2015-2016 Kriminalitätsstatistik für England und Wales eine separate Überschrift – ein deutliches Zeichen der sich verändernden Einstellungen.

Auch in Deutschland haben die Strafverfolgungsbehörden diesbezüglich aufgerüstet. Sie bieten spezielle Zentren auf Länderebene, die über entsprechende Fachkenntnisse und Netzwerke verfügen und vor allem den Bedürfnissen der betroffenen Unternehmen nach Kompetenz, Vernetzung und Diskretion Rechnung tragen können.

Das Bewusstsein für die Existenz und die Sinnhaftigkeit solcher Angebote ist jedoch bisher schwach. So vermeldete der FBI Internet Crime Report 2015 (mit Zahlen aus dem IC3 Report) nur 2.453 Ransomware Anzeigen für das betreffende Jahr – wahrscheinlich eine riesige Unterschätzung des wahren Maßstabs.

Sascha Pfeiffer empfiehlt: „Bis die öffentliche Berichterstattung und die Akzeptanz sich bessert, wird die Bekämpfung von Ransomware schwierig bleiben. Die Schätzungen der Ausmaße und Auswirkungen von Ransomware-Attacken verbleiben bei den IT-Security-Unternehmen. Deren Kompetenz liegt jedoch in der Informationsgewinnung zu den Angriffen und den Auswirkungen auf die IT – finanzielle und Image-Schäden der Betroffenen sind allein Sache der Ermittlungsbehörden.“

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
Christiane Capps, +49-174-3335550
Ulrike Masztalerz, +49-30-55248198
sophos@tc-communications.de