Großbritannien weltweit Ransomware-Hochburg, Deutschland kommt glimpflich davon

34% der im letzten halben Jahr weltweit erfassten Ransomware-Attacken fanden in Großbritannien statt, Deutschland belegt mit unter 1 Prozent Platz 7; PDFs und Office-Dokumente sind die häufigsten „Transportmittel" für Schadsoftware

Wiesbaden, 13. Juni 2017. Seit der WannaCry Attacke kommt das Thema Ransomware nicht mehr aus den Schlagzeilen. Unternehmen müssen schlichtweg akzeptieren, dass diese Form der Schadsoftware dauerhaft für Probleme sorgen und die tägliche Arbeit der IT-Sicherheitsexperten noch eine Weile dominieren wird.

Erpressertrojaner Cerber und Locky sind am aktivsten
SophosLabs nahm die produktivsten Ransomware-Familien und Angriffsvektoren über einen Zeitraum von sechs Monaten unter die Lupe und korrelierte die Ergebnisse zu einer grafischen Übersicht von Oktober 2016 bis April 2017. Die Analyse beinhaltet noch nicht den WannaCry-Ausbruch von Mitte Mai 2017. Zunächst nahmen die Experten spezifische Ransomware-Familien unter die Lupe: Cerber war für die Hälfte aller Aktivitäten während der Beobachtungsperiode verantwortlich – WannaCry dürfte in kommenden Analysen eine ähnliche Größenordnung erreichen. Auf Locky fallen immerhin noch knapp ein Viertel aller Aktivitäten (24%).

Der Erpressertrojaner Cerber – nicht ohne Grund nach dem mehrköpfigem Hund Cerberus benannt, der in der griechischen Mythologie die Unterwelt bewacht – durchlief zahlreiche Mutationen. Er wurde gezielt entwickelt, um Sandboxing und Antiviren-Programme zu umgehen. Eine Version verbreitete sich zum Beispiel via Spam-Mails, getarnt als Paket-Lieferankündigung. Die Ransomware Locky hat mittlerweile eine Historie in der Neubenennungen wichtiger Daten seiner Opfer, so dass diese mit dem Fortsatz .locky. enden. Wie bei Cerber auch haben sich die Vorgehensweise und das Aussehen über die Zeit immer wieder gewandelt.

Deutschland belegt Platz 7 auf der weltweiten Angriffskarte
Weltweit betreffen die größten Ransomware-Aktivitäten Großbritannien (34 Prozent), gefolgt von Belgien (20 Prozent), der Niederlande (14 Prozent) und den USA (13 Prozent). Nach Italien und Frankreich steht Deutschland mit einer anteiligen Bedrohungsquote von unter 1 Prozent an Platz 7. Nach der Überprüfung der Attackenfrequenz nahm sich SophosLabs die Verbreitungsmethoden und Evolutionskreisläufe von Malware vor: So kristallisieren sich verschiedene Verbreitungswege heraus: Spam, Web-Malvertisement (schadhafte Werbung auf einer Website) und Drive-by-Downloads, also das unbewusste Herunterladen von Malware.

Die vorherrschende Angriffstaktik von Ransomware war das Versenden von Email-Anhängen. Besonders beliebt dabei: PDFs und Office-Dokumente. Im Dezember

2016 ließ sich zudem ein auffallend starker Spam-Rückgang feststellen. „Das hat möglicherweise mit dem stillgelegten Botnet Necurs zu tun“, so Michael Veit, Security Experte bei Sophos. „Das heißt aber nicht, dass da nicht noch etwas vor sich hinschlummert und den nächsten Peak vorbereitet.“. Entsprechend wichtig ist die Prävention. Und das kann jeder:

1. Dem gesunden Menschenverstand vertrauen, bei Zweifeln keine Datei oder Emailanhänge öffnen.

2. Regelmäßige Backups seiner Daten erstellen und diese verschlüsselt hinterlegen.

3. Konstant Updates und Sicherheits-Patches einspielen.

4. Auf dem Gerät einstellen, dass Dateiendungen auf den ersten Blick zu sehen sind, so dass man sie nicht extra anklicken muss und damit möglicherweise Malware öffnet.

Über Sophos
Sophos ist führender Anbieter von Endpoint- und Network-Security-Lösungen der nächsten Generation. Als Pionier der Synchronized Security entwickelt Sophos sein innovatives Portfolio an Endpoint-, Netzwerk-, Verschlüsselungs-, Web-, E-Mail- und mobilen Security-Lösungen, die miteinander kommunizieren. Mehr als 100 Millionen Anwender in 150 Ländern verlassen sich auf Lösungen von Sophos mit hervorragendem Schutz vor anspruchsvollen Bedrohungen und Datenverlust. Sophos Produkte sind exklusiv über den weltweiten Channel mit mehr als 26.000 registrierten Partnern erhältlich. Sophos hat seinen Hauptsitz in Oxford, Großbritannien, und wird an der Londoner Börse unter dem Symbol "SOPH" öffentlich gehandelt. 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 +172 4536839
sophos@tc-communications.de