Mehr Internetangriffe

Im ersten Quartal 2015 gab es laut Kaspersky Lab weltweit um ein Drittel mehr Internetangriffe als im Vergleichszeitraum des Vorjahres. In Österreich stieg die Zahl der Angriffe um fast 80 Prozent.

Laut dem *Kaspersky Security Network* wurden im ersten Quartal 2015 insgesamt 2,2 Milliarden Angriffe auf Computer und mobile Geräte von *Kaspersky*-Kunden blockiert; das sind doppelt so viele wie im ersten Quartal 2014.

3,8 Millionen Webattacken erfolgten auf österreichische Kunden von *Kaspersky Lab* (erstes Quartal 2014: 2,1 Millionen). 23 Prozent der österreichischen *Kaspersky*-Nutzer wurden mindestens einmal im Internet attackiert.

Knapp 40 Prozent der weltweit von *Kaspersky Lab* geblockten Internetattacken erfolgten aus Russland. An zweiter Stelle folgen die USA (18 Prozent), an dritter die Niederlande (12,6 Prozent) und auf Rang vier Deutschland (6,9 Prozent).

Mobile Schädlinge. *Kaspersky Lab* entdeckte im ersten Quartal 2015 103.072 neue mobile Schädlinge; das sind 6,6 Prozent weniger als im ersten Quartal 2014. Im Vergleichszeitraum 2015 stieg die Zahl von Bank-Trojanern für mobile Geräte um 29 Prozent. Weltweit wurden 93 Millionen URL-Adressen als gefährlich eingestuft, um 14,3 Prozent mehr im Vergleich zum ersten Quartal 2014.

Phishing und Spam. Weltweit gab es zwischen Jänner und März 2015 eine Million Phishing-Angriffe mehr als im Vergleichszeitraum 2014. 37 Prozent der Phishing-Attacken haben es auf Kunden von Finanzorganisationen abgesehen – 19 Prozent auf Banken, 9,7 Prozent auf Online-Shops und

Angriffe im Internet nehmen weltweit zu. Der Softwareschutz sollte immer wieder aktualisiert werden.

8,4 Prozent auf Bezahldienste. Der Anteil von Spam-Mails am gesamten E-Mail-Verkehr lag im ersten Quartal des Jahres 2015 bei 59 Prozent, sechs Prozent weniger als im Vergleichszeitraum 2014. Die USA waren im Untersuchungszeitraum weltweit die Hauptverbreitungsquelle von Spam-Nachrichten (14,5 %). Es folgten Russland (7,3 %) und die Ukraine (5,7 %). Deutschland als Quelle für Spam-Nachrichten lag mit einem Anteil von 4,4 Prozent auf dem sechsten Platz.

Nutzer werden weiters über Top-Level-Domain-Anpassungen mit Hilfe von betrügerischen E-Mails attackiert. Das Anfang 2014 eingeführte Registrierungsprogramm für Top-Level-Domains ermöglicht es Organisationen, einen für sie sinnvollen Domain-Bereich (Domain Zone) zu wählen – beispielsweise „.work“ für Jobvermittlungsorganisationen oder „.science“ für wissenschaftliche Einrichtungen.

Auch Cyber-Kriminelle scheinen von dieser Option verstärkt Gebrauch zu machen. *Kaspersky Lab* entdeckte im ersten Quartal 2015 einen starken Anstieg an neuen Domain-Zones innerhalb der analysierten Spam-E-Mails. Neben den Beispielen mit dem Domain-Ende „.work“ und „.science“ waren zwischen Jänner und März auch die Endungen „.red“, „.pink“ und „.black“ beliebt. Der Grund: Werbung für asiatische Dating-Seiten.

„Versicherungen waren im ersten Quartal eines der zentralen Themen im E-Mail- beziehungsweise Spam-Traffic, auch was die Anzahl an sich verändernden Domain-Adressen in Massen-E-Mailings anbelangt. Dabei tauchen verschiedenste Arten wie Lebens-, Sport-, Gesundheits- oder Autoversicherungen auf“, sagt Tatyana Shcherbakova, Senior Spam Analyst bei *Kaspersky Lab*.

Typische Hinweise auf Spam-Mails und auf Phishing-Versuche sind ungefragt erhaltene Zusendungen von unbekannten und privaten Absendern. Oft enthalten diese E-Mails grammatikalische und orthografische Fehler. Inhalt und Betreff-Zeile stimmen nicht überein und die Empfänger werden nicht persönlich angesprochen. In den E-Mails wird oft nach persönlichen Daten gefragt, sie enthalten gefährliche Anhänge oder betonen eine hohe Dringlichkeit. Anwender sollten niemals sensible Daten wie Kreditkarteninformationen oder Account-Zugangsdaten preisgeben.

Sicherheitstipps. Neben dem Einsatz von Virenschutz-Software können Internetanwender Phishing-Versuche durch die Optimierung der Einstellungen des Spam-Filters des E-Mail-Anbieters abblocken.

Ein Risiko birgt das Anklicken von Links, das Öffnen von Anhängen und das Herunterladen von Software unbekannter Anbieter.

Alternativ können Nutzer die URL-Adresse der entsprechenden Webseiten eigenhändig in den Browser eintippen, um festzustellen, ob die Adresse von einer seriösen Quelle stammt oder nicht. Anwender sollten außerdem ihre E-Mail-Adressen möglichst nie öffentlich sichtbar im Internet hinterlassen und statt einer einzigen lieber mehrere zweckgebundene und Adressen ohne Namenscharakter verwenden. Damit können sie zum Beispiel Privates von Beruflichem oder Online-Shopping von der Nutzung sozialer Netzwerke trennen.

Anwender sollten nie auf Spam-Mails antworten, da sie ansonsten den Spammern die Existenz der E-Mail-Adresse bestätigen.

FOTO: FOTOLIA/TOMASZ ZAJDA