Was hilft bei Trojanern?

Serie Digitalisierung: Ein wichtiges Thema, mit dem sich auch Dachdeckerbetriebe beschäftigen müssen, ist IT-Sicherheit. Zunehmend werden auch sie Opfer von Hackerangriffen, oft in Form von Schadsoftware. Teil 4 unserer Digitalisierungsserie gibt Empfehlungen zum Schutz.

Claudia Büttner

Das BSI warnt vor Schadsoftware und gibt hilfreiche Tipps.

Vor einiger Zeit wütete der Trojaner Emotet in Deutschland, vor dem sogar das Bundesamt für Sicherheit in der Informationstechnik (BSI) warnte. Er galt als große Bedrohung, da er Ausfälle der kompletten IT-Struktur und somit Schäden in Millionenhöhe verursachte. Emotet verwendete zum Teil echte E-Mail-Adressen von Geschäftspartnern oder Kunden. Die Mails wirkten dadurch sehr offiziell (Pishing-Mails). Oft waren angeblich Rechnungen im Anhang, die dringend beglichen werden sollten. Hier ist äußerste Vorsicht geboten: Auf gar keinen Fall unbekannte Anhänge öffnen oder auf Links klicken, die in der Mail integriert sind. Denn ist der Computer erst einmal infiziert, lädt Emotet weitere Schadsoftware nach, wie zum Beispiel den Banking-Trojaner Trickbot.
Diese Schadprogramme führen zu Datenabfluss oder ermöglichen die vollständige Kontrolle über das IT-System. In mehreren Fällen hatte dies große Produktionsausfälle zur Folge, da ganze Unternehmensnetzwerke neu aufgebaut werden mussten. Für Privatanwender kann eine Infektion den Verlust von Daten, insbesondere wichtiger Zugangsdaten, bedeuten.

Empfohlene Schutzmaßnahmen des BSI

- Installieren Sie zeitnah bereitgestellte Sicherheitsupdates für Betriebssysteme und Anwendungsprogramme (Webbrowser, E-Mail-Clients, Office-Anwendungen etc.).
- Setzen Sie Antivirensoftware ein und aktualisieren Sie diese regelmäßig.
- Sichern Sie regelmäßig Ihre Daten (Backups).
- Richten Sie ein gesondertes Benutzerkonto auf dem Computer ein, um zu surfen und E-Mails zu schreiben.
- Öffnen Sie auch bei vermeintlich bekannten Absendern nur mit Vorsicht Dateianhänge von E-Mails (insbesondere Office-Dokumente) und prüfen Sie in den Nachrichten enthaltene Links, bevor sie diese anklicken. Bei einer verdächtigen E-Mail sollten Sie im Zweifelsfall den Absender anrufen und sich nach der Glaubhaftigkeit des Inhalts erkundigen.

Screenshot der SiBa-App

Tipps zur Schadenregulierung

- Informieren Sie Ihr Umfeld über die Infektion, denn Ihre Mailkontakte sind
- in diesem Fall besonders gefährdet.
- Ändern Sie alle gespeicherten und eingegebenen Zugangsdaten der betroffenen Systeme (zum Beispiel im Webbrowser).
- Die Schadprogramme nehmen teilweise tief greifende (sicherheitsrelevante) Änderungen am infizierten System vor. Sollte Ihr Rechner mit Schadsoftware wie Emotet infiziert sein, dann empfiehlt das BSI, diesen Rechner neu aufzusetzen.
- Umfangreiche Erläuterungen zur Schadsoftware und Maßnahmen zur Vorsorge sind hier abrufbar:
- http://bit.ly/BSI-Tipps-2018.

Sofortmaßnahmen per App

Hilfreich ist die App SiBa: Das Sicherheitsbarometer stellt Meldungen zu aktuellen Risiken für den digitalen Alltag bereit und gibt direkt passende Sicherheitstipps. Kurz und bündig werden Sofortmaßnahmen aufgezeigt sowie konkrete Schutzmöglichkeiten.
Die Risiken sind durch eine Ampelkennzeichnung leicht zu erkennen. Über außerordentliche Gefahren informiert die App durch Push-Nachrichten direkt auf das Smartphone. Die Smartphone-App ist für Android, Apple iOS und Windows Phone in den jeweiligen App-Stores erhältlich.

Kontaktdaten der Zentralen Ansprechstellen -Cybercrime der Länder und des Bundes*		
Land/Bund	Telefonnummer	E-Mail-Adresse
Bundeskriminalamt	0611 55-15037	SO41-NKC@bka.bund.de
Baden-Württemberg	0711 5401-2444	cybercrime@polizei.bwl.de
Bayern	089 1212-3300	zac@polizei.bayern.de
Berlin	030 4664-924924	zac@polizei.berlin.de
Brandenburg	03334 388-8686	zac@polizei.brandenburg.de
Bremen	0421 362-19820	cybercrime@polizei.bremen.de
Hamburg	040 4286-75455	zac@polizei.hamburg.de
Hessen	0611 83-8377	zac.hlka@polizei.hessen.de
Mecklenburg-Vorpommern	03866 64-4545	cybercrime.lka@polmv.de
Niedersachsen	0511 26262-3804	zac@lka.polizei.niedersachsen.de
Nordrhein-Westfalen	0211 939-4040	cybercrime.lka@polizei.nrw.de
Rheinland-Pfalz	06131 65-2565	lka.cybercrime@polizei.rlp.de
Saarland	0681 962-2448	cybercrime@polizei.slpol.de
Sachsen	0351 855-3226	zac.lka@polizei.sachsen.de
Sachsen-Anhalt	0391 250-2244	zac.lka@polizei.sachsen-anhalt.de
Schleswig-Holstein	0431 160-4545	cybercrime@polizei.landsh.de
Thüringen	0361 341-1425	cybercrime.lka@polizei.thueringen.de

Nicht neu, aber lästig: Kettenbriefe

Auch dies eine lästige Nebenerscheinung der digitalen Welt: Kettenbriefe über Whatsapp oder Facebook. Sie sind nicht unbedingt gefährlich, aber überflüssig und -tragen unnötig zur Verunsicherung bei. Aktuell sorgt gerade mal wieder ein solcher auf Facebook für Unruhe, wie auf der Webseite www.onlinewarnungen.de zu lesen ist. Facebook sei jetzt eine öffentliche Einrichtung, steht in diesem Kettenbrief.

Und wer nicht möchte, dass seine Fotos, Beiträge und Nachrichten von Facebook öffentlich genutzt werden, der solle einen Text posten, der folgendermaßen beginnt: „Lieber sicher sein, als dass es einem leidtut. Ein Anwalt hat uns empfohlen, dies zu posten. Gut genug für mich. Die Verletzung der Privatsphäre kann gesetzlich bestraft werden (...)."

Das Prinzip ist nicht neu, funktioniert aber immer wieder. Das zeigt die Angst der Facebook-Nutzer um ihre Daten. Aber ob ein Nutzer einen mehr oder weniger sinnfreien Text kopiert und postet oder nicht, interessiert weder Facebook noch hat das irgendeine Bedeutung hinsichtlich datenschutzrechtlicher Belange.
Fazit: Solche Kettenbriefe getrost ignorieren! //

Achtung: Aktuell werden Fake-Mails versandt – getarnt als Abmahnschreiben wegen angeblicher DSGVO-Verstöße bei Facebook oder der Webseite. Besonders tückisch ist dies, weil es mit Absenderadressen von zum Teil echten Anwaltskanzleien geschieht. Diese Anhänge bitte nicht öffnen. Details dazu hier: http://bit.ly/fake-mail-2019.

Autorin
Claudia Büttner ist
Pressesprecherin des ZVDH.