Achtung: Gefährliche Trojaner-Welle

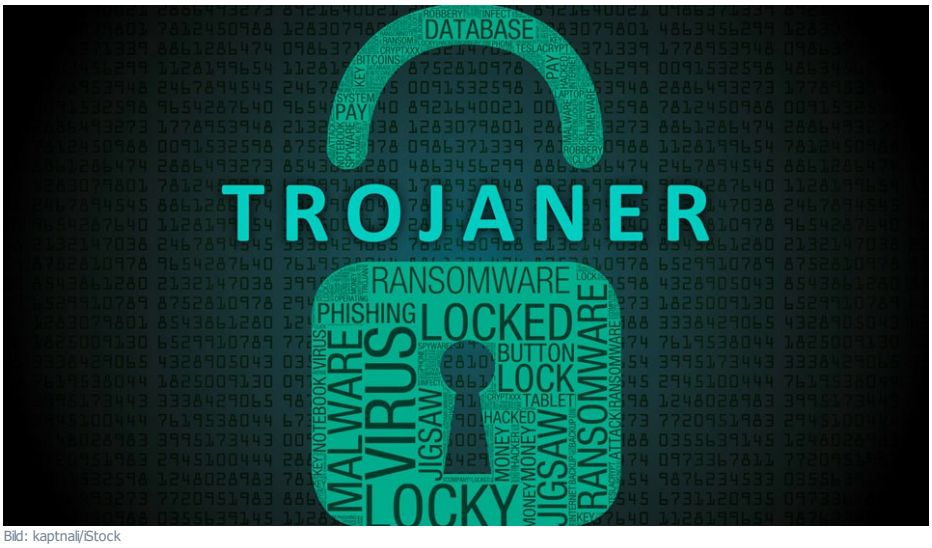

Bild: kaptnali/iStock

Liebe DGV-Mitglieder, aktuell werden Phishing-Mails versendet, welche sowohl der DGV, als auch einige Mitgleider bereits erhalten haben. Nachstehend finden Sie einen Beitrag von Jürgen Schmidt (erschienen auf heise.de), der Sie über die Gefahren und das richtige Verhalten informiert.

Achtung Dynamit-Phishing: Gefährliche Trojaner-Welle Emotet legt ganze Firmen lahm

> *"Eine Cybercrime-Gang legt derzeit in Deutschland ganze Firmen lahm. Die Schäden erreichen schon in einzelnen Fällen Millionenhöhe; der Gesamtumfang lässt sich noch nicht überblicken. Der Verursacher ist Emotet – ein Trojaner, der mit äußerst gut gemachten Phishing-Mails ins Haus kommt und dabei kaum von echten Mails zu unterscheiden ist.*
>
> *Die Emotet-Mails mit Trojaner-Anhang stammen scheinbar von Kollegen, Geschäftspartnern oder Bekannten. CERT-Bund und Polizei-Behörden berichten von einer großen Zahl von Infektionen vor allem bei Unternehmen und Behörden; allein der Zentralen Ansprechstelle Cybercrime des LKA Niedersachsen liegen dutzende aktuelle Vorfälle bei Firmen vor.*
>
> *Die Kriminellen haben sich offenbar Methoden und Techniken der staatlich geförderten Hacker-Gruppen abgeschaut: "Emotet ist nach unserer Einschätzung ein Fall von Cyber-Kriminalität, bei der die Methoden hochprofessioneller APT-Angriffe adaptiert und automatisiert wurden", erklärt BSI-Präsident Arne Schönbohm die neuartige Qualität der Angriffe. Konkrete Vorbilder für die neuen Cybercrime-Aktivitäten sind Spear-Phishing und das sogenannte Lateral Movement nach einer Infektion.*
>
> ### *Dynamit-Phishing*
>
> *Beim Spear Phishing schicken die Angreifer sehr gut auf eine Zielperson zugeschnittene E-Mails, mit der Absicht, diese dazu zu verleiten, den Mail-Anhang zu öffnen. So dringen sie selbst in die gesicherten Netze von Regierungen und Rüstungskonzernen ein.*
>
> *Emotet sammelt seit Monaten bei seinen Opfern Informationen darüber, wer in einer Firma mit wem kommuniziert. Darüber hinaus greifen die letzten Versionen auch den Inhalt der Mails ab. Damit lassen sich Phishing-Mails bauen, die nahezu perfekt an das normale Kommunikationsverhalten in einer Firma angepasst sind. Anders als beim Spear-Phishing werden die Mails jedoch nach wie vor automatisiert erstellt und in großer Zahl verschickt. Vielleicht sollte man angesichts Verbreitung und Wirkung also eher von "Dynamit-Phishing" reden.*
>
> ### *Angriff im Netz*
>
> *Aktuelle Emotet-Mails enthalten eine Doc-Datei mit Makros. Deren Abarbeitung muss der Empfänger nach dem Öffnen in Microsoft Word erst gestatten – was offenbar immer wieder geschieht. Dann wird der Rechner über eingebettete PowerShell-Kommandos infiziert und weitere Schad-Software aus dem Internet nachgeladen.*
>
> *Den erwähnten Schaden bis zum Lahmlegen der gesamten IT verursacht aber nicht die Erstinfektion. Vielmehr versucht sich Emotet nach dem Vorbild der APT-Hacker zunächst im Netz auszubreiten (Lateral Movement). Dazu nutzt es auf dem Rechner abgeerntete Zugangsdaten und auch einen Exploit, der aus den Geheimlabors der NSA stammt. Mit EternalBlue kaperten die US-Hacker mit Regierungsauftrag über Jahre hinweg ganze Firmennetze. Jetzt nutzen die Emotet-Gauner den Exploit und finden offenbar immer noch Opfer, die den von Microsoft bereitgestellten Patch nicht eingestellt haben.*
>
> ### *Schutz*
>
> *Um sich vor Emotet-Infektionen zu schützen, muss man auf eine Kombination von Awareness bei den Mitarbeitern und technischen Maßnahmen setzen. Ein Kernpunkt der Infektion ist die Ausführung von Makros, die für Doc-Dateien, die man per E-Mail erhält, nur selten wirklich erforderlich ist. Administratoren sollten dies etwa über Gruppenrichtlinien so weit wie möglich verbieten. In der frei verfügbaren Open-Source-Lösung LibreOffice funktionieren die Emotet-Makros übrigens nicht.*

Informationen zum Text

10. Dezember 2018
IT&Datenschutz

Weiterführende Links

Beitrag auf heise.de lesen

> *Darüber hinaus sollte man Maßnahmen zur Stärkung des Sicherheitsniveaus im Firmennetz ergreifen, die die Ausbreitung verhindern oder zumindest einschränken. Das Einspielen aktueller Sicherheits-Updates ist die Grundvoraussetzung dafür. Das BSI gibt weitere konkrete Tipps zum Schutz vor Emotet für Bürger und im Rahmen der Allianz für Cybersicherheit auch für Administratoren von Firmennetzen."*

Autor: Jürgen Schmidt

Quelle: heise.de (Stand: 11. Dezember 2018)
