Schotten dicht?

Behörden gehen vor Emotet in Deckung

(BS/Uwe Proll/Benjamin Stiebel) Um ihre IT-Systeme vor Infektionen zu schützen, greifen einige Behörden zu drastischen Mitteln und blockieren den Empfang von URLs oder Anhängen in E-Mails. Für die Sicherheit ist das ein Plus, für die alltägliche Arbeit der Beschäftigten teils eine Katastrophe. Anlass war eine neue Angriffswelle mit der Schadsoftware Emotet vor Weihnachten. Dieses Mal war auch der Bund betroffen. Nun stellt sich die Frage, wie in der Zukunft mit den Risiken umzugehen ist.

In welcher Bundesbehörde der schwere Vorfall seinen Anfang genommen hat, darüber herrscht Schweigen ("Opferschutz"). Klar ist jedoch, dass dieses erste Eindringen Nebenwirkungen für die gesamte Bundesverwaltung hatte. Im Namen mehrerer bereits befallener Bundesbehörden wurden weitere schadhafte Mails verschickt. Folge waren weitere Infektionen. Betroffen waren über den Umweg auch nachgeordnete Behörden im Geschäftsbereich des Bundesinnenministeriums (BMI), so das Technische Hilfswerk. Auch das Ministerium selbst blieb nicht verschont. Über Art und Ausmaß der Schäden lässt sich im Moment nichts Sicheres sagen. Im Zuge der Bereinigung mussten teils IT-Systeme heruntergefahren werden.

Auch öffentliche Einrichtungen in Hessen hatten um den Jahreswechsel mit Emotet zu kämpfen. Kurz vor Weihnachten ist die Stadtverwaltung Frankfurt am Main offline gegangen, um eine Verbreitung des Schädlings einzudämmen. Einfallstor war hier ein Rechner in einem Bürgeramt. Auch in Bad Homburg und der Stadt Alsfeld sind zeitweise sämtliche Server heruntergefahren worden. Die Ursache mit hoher Wahrscheinlichkeit auch hier: Emotet. Die Universität Gießen hatte einen schweren Befall schon Anfang Dezember 2019 festgestellt. Reparaturarbeiten dauern dort noch an und werden sich voraussichtlich noch bis in den Februar hinziehen.

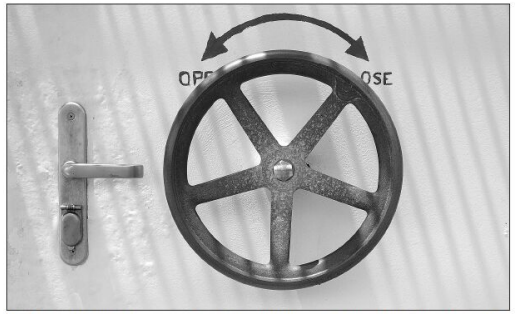
In Bayern waren das Klinikum Fürth und die Stadtverwaltung Nürnberg betroffen. Während letztere glimpflich davongekommen ist, konnten im Krankenhaus vorübergehend keine Patienten im Rahmen des Rettungsdienstes aufgenommen werden. Planbare Operationen wurden verschoben. In einer früheren Angriffswelle im September waren unter anderem die niedersächsische Stadt Neustadt am Rübenberge, die Medizinische Hochschule Hannover und das Berliner Kammergericht betroffen gewesen.

Sicher durch Abschottung?

Nach den jüngsten Fällen reagierten Teile der öffentlichen Verwaltung mit restriktiven Richtlinien beim Empfang externer Mails. Im BMI und Teilen des nachgeordneten Bereichs werden Links aus Nachrichten entfernt und durch einen Hinweis ersetzt: "Die URL wurde aus IT-Sicherheitsgründen entfernt." Wenn angehängte Dokumente Makros, Skripte oder ausführbaren Code enthalten, wird die Mail nicht durchgestellt. Außerdem dürfen Anhänge keine aktiven Links enthalten. Damit sind auch Informationssammlungen, Strategie- oder Positionspapiere oder Info-Mailings nicht zustellbar. Das betrifft auch den behördenübergreifenden Mail-Verkehr im IVBB (Informationsverbund Berlin-Bonn). Zwar gilt das Regierungsnetz selbst als sicher. Offenbar kann oder möchte man aber derzeit Mails angeschlossener Stellen nicht vertrauen.

Ähnliche Regeln wie das BMI setzt auch der IT-Dienstleister IT.NRW, der für Kommunikation der Landesverwaltung in Nordrhein-Westfalen zuständig ist. Bei der Polizei des Landes, die ihre IT-Infrastruktur separat betreibt, gelten keine Einschränkungen. Auch in Niedersachsen gibt es keine einheitliche Linie. Die Finanzverwaltung geht besonders restriktiv vor. Dort werden alle Mails mit Links oder angehängten Microsoft-Office-Dokumenten generell geblockt. Eine Information des Absenders erfolgt nicht. Die Einschränkung wird explizit mit dem Schutz vor Emotet begründet. In anderen Teilen der niedersächsischen Landesverwaltung gilt das nicht. Mails werden durchgelassen, Mitarbeiter erhalten nur einen Warnhinweis bei Nachrichten von außerhalb, dass sie auf keine Links klicken sollten.

Durch die IT-Sicherheitsbrille besehen, sind die Maßnahmen geeignet, Risiken deutlich zu senken. Schließlich sind E-Mails mit schadhaften Links oder Anhängen nach wie vor das Einfallstor Nummer eins für Viren, Trojaner oder Ransomware. "Nicht nur Unbedarfte fallen leicht auf gut gemachte Phishing-Mails rein. Keiner sollte davon ausgehen, dagegen gefeit zu sein", warnt *Joachim Weide*, Sicherheitsexperte bei G4C (German Competence Centre against Cyber Crime). In dem Verein vernetzen sich Unternehmen aus der Finanz- und IT-Sicherheitsbranche für einen vertrauensvollen Austausch. Das Bundeskriminalamt (BKA) und das Bundesamt für Sicherheit in der Informationstechnik (BSI) sind Kooperationspartner. Die Entscheidung, Links zu blockieren, findet *Weide* in der gegenwärtigen Situation nachvollziehbar. Sie hat aber ihren Preis.



Nach erneuten Infektionen mit der Schadsoftware Emotet setzen einige Behörden nun auf Abschottung. E-Mails mit Links oder Anhängen werden abgewiesen oder um die potenziell gefährlichen Inhalte erleichtert.

Foto: BS/Attapol, stock.adobe.com

Von Mitarbeitern aus dem Geschäftsbereich des BMI ist zu hören, dass normale Arbeitsabläufe massiv gestört sind. Die behördenübergreifende gemeinsame Arbeit an Dokumenten ist erschwert. Genau wie der Informationsaustausch und die Zusammenarbeit mit Bürgern, Verbänden, Vereinen oder Unternehmensvertretern. Sowohl Dritten als auch den Mitarbeitern selbst sind die Einschränkungen bei der Kommunikation nur schwer zu vermitteln. Manche geben Links derweil über Umwege weiter, zum Beispiel als Bilder. Nutzer müssen die URLs dann aber händisch im Browser eingeben. Viele Beschäftigte haben sich zunächst über die unzeitgemäße Arbeitsweise beschwert. Mittlerweile können zumindest PDFs empfangen werden. Diese werden in Bilder umgewandelt und dabei von sämtlichen Links und aktiven Inhalten befreit.

Doch wo liegt die Alternative? "Anhänge und Links auf Schadsoftware zu untersuchen, ist schwierig, aber durchaus möglich", sagt *Weide*. Die meisten Schädlinge würden durch vernünftig konfigurierte Lösungen auf dem Stand der Technik herausgefiltert. "Aber hundertprozentigen Schutz gibt es nirgendwo", stellt der Fachmann klar.

Tausendsassa Emotet

Das Problem mit Emotet: Der von BSI-Präsident *Arne Schönbohm* schon im Dezember 2018 als "weltweit gefährlichste Schadsoftware" bezeichnete Trojaner ist nicht nur besonders erfolgreich darin, auch in solide abgesicherten Netzwerken Fuß zu fassen. Die möglichen Schäden sind auch besonders weitreichend. Eine automatisierte Auswertung des Mail-Verkehrs bereits betroffener Nutzer erlaubt Emotet die Ableitung persönlich und authentisch wirkender Phishing-Mails im Namen von Kollegen, Geschäftspartnern und sonstigen Kontakten. Grundlage sind Methoden, die zuvor nur von professionellen und langfristig durchgeführten Angriffen auf besonders kritische Ziele bekannt waren.

Einmal auf dem Rechner, kann Emotet weitere Schadsoftware nachladen, mit der Zugangsdaten abgezogen oder ein vollständiger Fernzugriff auf Systeme realisiert werden kann. Typisch ist eine Verschlüsselung von Daten mittels Ransomware und die Erpressung von Lösegeld. Anders als bei früheren Kampagnen werden zumeist keine Pauschalforderungen gestellt. Vielmehr sehen sich die Täter häufig zunächst in den kompromittierten Netzwerken um und passen das Lösegeld individuell an Zahlungsfähigkeit und Sensibilität der vorgefundenen Daten und Systeme an. Von Emotet nachgeladene Software kann zur automatisierten Weiterverbreitung auch verschiedene Sicherheitslücken nutzen, die in nicht optimal abgesicherten Netzwerken vorkommen. Auch den "EternalBlue" getauften Windows-Exploit, der schon 2017 die massenhafte Verbreitung der Ransomware WannaCry ermöglicht hatte. Die potente Cyber-Waffe war ursprünglich von der NSA entwickelt und für eigene Zweck genutzt worden – bis sie kriminellen Hackern in die Hände fiel.

Dass Emotet technisch so mächtig und vielseitig ist, macht es besonders beliebt. Im Sommer 2019 gab es bereits über 30.000 Varianten. Nach wie vor kommen täglich neue dazu und diese können dann eben nicht immer sofort durch Standard-Virenscanner erkannt werden. "Darum ist die Sensibilität bei den Nutzern nach wie vor der wichtigste Aspekt," sagt G4C-Vertreter *Weide*.

Beil oder Florett?

Wie geht es nun weiter? Anhänge und Links per se zu blocken, ist der falsche Weg. E-Mail ist der vorherrschende Kommunikationsweg für die Arbeit in allen Branchen und Sektoren. Behörden brauchen intensiven Kontakt mit Dritten und das Gros (80% schätzen Experten) der relevanten Inhalte im Mailverkehr kommt in Form von Anhängen daher. Das Ziel kann nicht Minimierung von Risiken durch größtmögliche Einschränkung sein. Vielmehr muss eine Verhältnismäßigkeit zwischen Sicherheit und Anwendbarkeit erreicht werden. Das gebieten schon die immer wieder erneuerten Bekenntnisse zu mehr zeitgemäßer, digitaler Verwaltung. Statt die Verbindungen mit dem Beil zu kappen *(vgl. die Karikatur auf der Titelseite)*, muss mit dem technischen Florett reagiert werden. So gibt es Sandboxing-Lösungen, mit denen – eine durchdachte Konfiguration und Einbettung in die Systemlandschaft vorausgesetzt – sicher gesurft werden kann. Der vom BSI mitentwickelte Browser in the Box ist nur ein Beispiel. Andere Verfahren basieren auf Whitelisting von Links. Klickt der Nutzer einen Link, erfolgt vor der eigentlichen Anfrage im Hintergrund eine gesicherte Testanfrage. Wird kein verdächtiges Verhalten festgestellt, wird der Zugriff durchgelassen, die Maschine beobachtet den Netzverkehr aber weiter. Für den Nutzer bedeutet das ledigilich eine kleine Verzögerung. Erst wenn durch verschiedene Nutzer eine gewisse Anzahl von Verbindungen zu der Adresse ohne Auffälligkeiten aufgebaut worden ist, kommt der Link auf eine Whitelist und kann auch ohne gesonderte Testanfrage geöffnet werden.

Dass normales Arbeiten und hohes Sicherheitsniveau sich verheiraten lassen, zeigen positive Beispiele aus der Bundesverwaltung. Beim BSI wurde anders als beim BMI nach der jüngsten Emotet-Welle kein konkreter Handlungsbedarf gesehen. Die Infrastruktur der Cyber-Sicherheitsbehörde ist gut abgesichert, Das Risiko eines Durchdringens von Schadsoftware durch die Analyse-Systeme ist gering. Auch im Geschäftsbereich des Bundesministeriums der Verteidigung (BMVg) vertraut man nach wie vor den eigenen Sicherheitssystemen. Alle Mails werden geöffnet und auf Herz und Nieren gescannt. Reguläre Links und Anhänge können entsprechend unberührt durchgelassen werden.

Das BMVg ist ein Musterbeispiel für Standardisierung und Zentralisierung in der IT. Darin liegt die materielle Voraussetzung für ein hohes IT-Sicherheitsniveau. Es ist kein Zufall, dass der Bundesrechnungshof in seiner jüngsten Kritik zum Stand der IT-Konsolidierung des Bundes insbesondere auch die Vernachlässigung der IT-Sicherheit gerügt hat. Keine Frage: Die Verantwortlichen haben das Thema auf dem Schirm. Die Verwaltung ist sichtlich um sicheren IT-Betrieb bemüht. Das zeigen auch die jüngsten Reaktionen. Aber solange es nicht gelingt, eine zentrale und standardisierte IT-Infrastruktur zu schaffen, wird ein konsistentes IT-Sicherheitsmanagement auf hohem Niveau schwer zu erreichen sein. Nur wer seine Strukturen kennt, kann Risiken gut einschätzen und eindämmen. Nur mit klaren und standardisierten Strukturen können Standard-Maßnahmen wie Patchmanagement und Back-Up-Pflege ordentlich funktionieren.