IT-Sicherheitsvorfall beim DVGW – Chronologie eines Angriffs

Ein IT-Sicherheitsvorfall hat am 19. September 2019 dazu geführt, dass große Teile der IT-Infrastruktur des DVGW heruntergefahren werden mussten. In der Folge waren sowohl die Hauptgeschäftsstelle in Bonn als auch die Außenstellen für ca. 36 Stunden per E-Mail nicht mehr erreichbar. Grund für den großflächigen Ausfall war eine mutmaßliche Infektion des IT-Systems mit der Schadsoftware „Emotet". Der Beitrag zeichnet die Chronologie des Vorfalls nach, erläutert die Mechanismen des Angriffs und beschreibt, welche Maßnahmen das IT-Team des DVGW seither getroffen hat.

von: Rainer Stecken (DVGW Service & Consult GmbH)

Erste Hinweise auf eine mögliche Infektion mit Schadsoftware gingen bereits am Abend des 18. Septembers 2019 beim IT-Team des DVGW ein. Mehrere Partner und Kunden hatten auffällige E-Mails von DVGW-Mitarbeitern erhalten, die jedoch allesamt auf bereits existierende Mailkonversationen Bezug nahmen und an diese anknüpften – für die Verantwortlichen ein erster Hinweis darauf, dass das IT-System des DVGW von der Schadsoftware „Emotet" befallen sein könnte. Diese liest die Mail-Inhalte und Kontaktdaten aus den Mailprogrammen bereits betroffener Nutzer aus und generiert daraus Spam-Mails – eine besonders perfide Vorgehensweise, da diese Nachrichten als vermeintliche Antworten auf tatsächliche E-Mails versendet werden und in den meisten Fällen u. a. auch eine korrekte Anrede enthalten. Ziel der Mails ist es, den angeschriebenen Benutzer zum Öffnen präparierter Dateien (z. B. im Word-Format) zu bewegen und somit auch dessen Computer mit der Schadsoftware zu infizieren.

Auf der Suche nach dem „Patienten 0"

Im konkreten Fall des DVGW zitierten die auffälligen E-Mails Konversationen aus dem Frühjahr. Das IT-Team schloss daraus, dass bereits zu einem früheren Zeitpunkt Daten von einem System des DVGW oder eines Partners bzw. Kunden abgeflossen sein mussten. Nur wenige Minuten nach dem Bekanntwerden des Vorfalls informierten die Verantwortlichen den DVGW-Vorstand und holten sich von diesem die Erlaubnis ein, das betroffene IT-System vom Netz zu trennen. Bei dieser Vorgehensweise handelt es sich um eine bewährte Standardmaßnahme, die es erlaubt, das eigene System eingehend zu untersuchen und die Infektionsherde gezielt einzugrenzen. Tatsächlich konnte das IT-Team relativ schnell den „Patienten 0", also den mutmaßlich zuerst infizierten Computer, lokalisieren. Mithilfe hinzugerufener IT-Forensiker wurde das gesamte IT-System anschließend auf einen Emotet-Befall hin untersucht – allerdings ohne Ergebnisse. Eine Erklärung für diesen Negativbefund ist, dass das regelmäßige, zeitnahe Aktualisieren der Schutzmechanismen und aller Rechner eine Infektion der Nachbarrechner verhindert hat, weil Schwachstellen für weitere Angriffe auf die umliegenden Systeme rechtzeitig geschlossen wurden. Denkbar ist aber auch, dass es nie eine Infektion auf weiteren Computern des DVGW gegeben hat, sondern dass die Daten einmalig von einem Rechner nach außerhalb abgeflossen sind. Nach 36 Stunden war das IT-System dann wieder am Netz und konnte regulär verwendet werden.

HINTERGRUND

Die IT-Infrastrukturen des DVGW gliedern sich in zwei Teile: Der erste bietet für die Mitarbeiter in der Hauptgeschäftsstelle und den Niederlassungen die normalen Office-Funktionalitäten und enthält u. a. auch den Mailserver. Der zweite Teil stellt über ein externes Rechenzentrum Web-Angebote bereit, die bei Bedarf und unter Nutzung von Sicherungsmechanismen aus dem internen Netz mit neuen Daten versorgt werden. Beide Teile laufen getrennt voneinander und sind jeweils mit einem empfehlungskonformen Firewall-Konzept ausgestattet. Zudem verfügt jedes System über eine stets aktuelle Virenschutzlösung; Patches und Updates der Softwarehersteller werden zeitnah auf allen Systemen ausgerollt.

Weitere Maßnahmen

Parallel zu den beschriebenen Direktmaßnahmen informierte das IT-Team das Bundesamt für Sicherheit in der Informationstechnik (BSI), die Zentrale Ansprechstelle Cybercrime (ZAC NRW) und die Kriminalpolizei Bonn. Das BSI gab im Rahmen der Spurensuche wichtige Hinweise, wie eine Infektion detektiert und nachgewiesen wer-

den kann, und bot Helfer zur Forensik an. Darüber hinaus wurde auch der Datenschutzbeauftragte umgehend von den Vorgängen in Kenntnis gesetzt, er wiederum meldete den Vorfall an die Datenschutzbehörden in NRW. Zu guter Letzt informierte das IT-Team den Hersteller der auf dem IT-System verwendeten Virenschutzsoftware; dieser teilte mit, dass die aktuelle Emotet-Variante erst durch ein am 19. September verfügbares Update der Virendefinitionen detektiert werden konnte.

Kommunikation nach Innen und Außen

Da sich der Sicherheitsvorfall am Abend des 18. Septembers ereignete, konnte das IT-Team die DVGW-Mitarbeiter in den verschiedenen Zweigstellen erst am nächsten Tag über den Vorgang informieren, dies geschah (aus offensichtlicher Ermangelung digitaler Kommunikationswege) durch gedruckte Warnzettel an relevanten Stellen (wie z. B. den Stationen zur Zeiterfassung und den Zugängen zu den Hausfluren). Auch die Mitarbeiter, die sich zu diesem Zeitpunkt im Homeoffice befanden, setzte man telefonisch in Kenntnis. Da die Untersuchung des IT-Systems zu diesem Zeitpunkt noch im Gange war, erging an die Mitarbeiter die strikte Anweisung, die Computer nicht einzuschalten und keine VPN-Verbindungen aufzubauen.

Der Sicherheitsvorfall hat verdeutlicht, dass die externe Notfallkommunikation derzeit noch ausbaufähig ist: Externe Partner konnten nur aufgrund der Tatsache, dass die DVGW-Mitarbeiter nicht per Mail zu erreichen waren, auf einen IT-Vorfall schließen; genauere Informationen erhielten sie jedoch nicht. An dieser Stelle möchte das IT-Team in Zukunft eine aktivere Krisenkommunikation etablieren und z. B. über die BSI-Verteiler KRITIS/Gas und KRITIS/Wasser frühzeitig über eventuelle Vorkommnisse informieren. Hierzu werden die Verantwortlichen neue Kommunikationspläne erstellen bzw. bereits bestehende Pläne entsprechend erweitern. Durch das Teilen von relevanten Informationen sollen dann auch eventuelle Schäden außerhalb der eigenen Organisation vermieden werden.

Zusammenfassung und Ausblick

Das Team des DVGW war innerhalb von Minuten in der Lage, aus den eingehenden Nachrichten auf die konkrete Gefahr – in diesem Fall die Schadsoftware Emotet – zu schließen und die notwendigen Notfallmaßnahmen schnell einzuleiten. Die Zusammenarbeit innerhalb des IT-Teams lief dabei reibungsfrei, und auch die Behördenkontakte waren bekannt und wurden umgehend genutzt. Schwieriger gestaltete sich hingegen die Informierung der DVGW-Mitarbeiter, da der Befall außerhalb der Arbeitszeit festgestellt wurde und nicht jeder so schnell erreicht werden konnte, wie dies wünschenswert gewesen wäre. Auch in der externen Kommunikation gibt es Verbesserungsbedarf: Die nach dem Vorfall eingeleiteten Maßnahmen sollen sicherstellen, dass der DVGW in zukünftigen Krisenfällen aktiv auf alle Mitglieder und Partner zugehen kann. Eine weitere Lehre aus dem Vorfall ist, dass in Zukunft alle Mitarbeiter im Rahmen von Informationssicherheits-Unterweisungen über mögliche Gefahren informiert werden. Der DVGW hat aus dem Befall mit Schadsoftware gelernt und setzt bereits jetzt entsprechende Maßnahmen um, die mittelfristig in der Einführung der Norm ISO/IEC 27001 münden sollen. ■

CHRONOLOGIE

18. September 2019, 17:30 Uhr:
Erste Meldungen über auffällige E-Mails erreichen das IT-Team.

18. September 2019, 17:40 Uhr:
Das technische Team diagnostiziert eine mögliche Infektion mit der Schadsoftware „Emotet“, das IT-System wird vom Internet getrennt.

18. September 2019, ab 17:45 Uhr:
Der DVGW-Vorstand und die Leitungsebene werden über den Vorfall unterrichtet, zudem informiert das IT-Team das BSI, die Zentrale Ansprechstelle Cybercrime ZAC NRW und die Kriminalpolizei Bonn. Parallel beginnen die Vorbereitungen, um die DVGW-Mitarbeiter über den Vorfall zu informieren.

19. September 2019, ab 07:00 Uhr:
Das Krisenteam tritt zusammen und bereitet die weiteren erforderlichen Schritte vor.

19. September 2019, ab 10:00 Uhr:
Die Rechnerüberprüfung mit Forensik-Unterstützung beginnt.

20. September 2019, 10:00 Uhr:
Mit Ausnahme einer Niederlassung wird die Nutzung des Netzes wieder freigegeben.

20. September 2019, ab 15:00 Uhr:
Das komplette Netz ist wieder voll betriebsbereit.

Der Autor

Rainer Stecken ist Berater für Informationssicherheit bei der DVGW Service & Consult GmbH.

Kontakt:
Rainer Stecken
DVGW Service & Consult GmbH
Josef-Wirmer-Str. 1–3
53123 Bonn
Tel.: 0228 9188-669
E-Mail: stecken@dvgw-sc.de
Internet: www.dvgw-sc.de