Cyber-Sicherheit: E-Mails gelten als eine der größten Angriffsflächen für die Cyber-Kriminalität, etwa zur Einschleusung von Schadsoftware oder zu Vermögensbetrügereien.

Gefährliche Anhänge

Der Bayerische Verband für Sicherheit in der Wirtschaft e.V. veranstaltete zusammen mit dem Bayerischen Landeskriminalamt, Zentrale Ansprechstelle Cybercrime, am 13. Jänner 2022 ein Online-Seminar zum Thema E-Mail-Sicherheit.

Andreas Bauer und Michael Weber von der *Zentralen Ansprechstelle Cybercrime (ZAC; zac@polizei.bayern.de)* bezeichneten E-Mails als eine der größten Angriffsvektoren für die Cyber-Kriminalität, etwa zur Einschleusung von Schadsoftware oder zu Vermögensbetrügereien. Sie zeigten an Hand von anonymisierten E-Mails die Vorgangsweisen der Täter auf und gaben Tipps zum Erkennen und zur Vermeidung gefährlicher E-Mails.

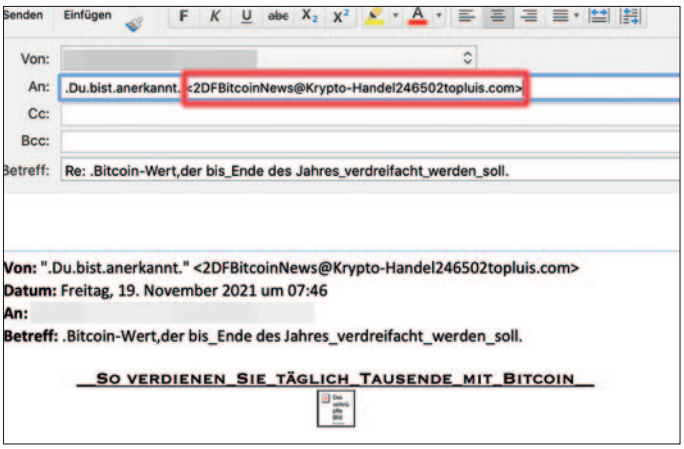
Die E-Mail gebe es seit etwa 40 Jahren. Damals habe es ausgereicht, dass eine Mail den Empfänger erreicht, die Sicherheit des Mailverkehrs im Sinn von Security sei laut den Referenten damals kaum im Fokus gestanden. Bei von E-Mails ausgelösten Schadfunktionen sei ein aktives Handeln erforderlich. Man werde dazu aufgefordert, etwa einen Button zu drücken oder einen Link anzuklicken. Ferner würde eine besondere Dringlichkeit behauptet und der Adressat damit unter Druck gesetzt. Vor Rechtschreibfehlern strotzende, in schlechtem Deutsch oder Englisch abgefasste und somit von vornherein verdächtig erscheinende Mails seien durch raffinierte, dem Corporate Design angepasste, auf den ersten Blick unverdächtig erscheinende Zusendungen ersetzt worden.

In einem Beispielfall wurde der Adressat darauf aufmerksam gemacht, dass er offenbar ein ihm zugesendetes Vertragsdokument, das in einem Punkt noch näher zu besprechen wäre, nicht erhalten habe. Er könne sich das Dokument auf der *Adobe Cloud* ansehen. Stattdessen wurde er durch Anklicken dieses Buttons auf die *Microsoft* 365-Seite umgeleitet, auf der er seine E-Mailadresse und Kennwort eingab. Dadurch war es den Angreifern möglich, sich in der IT des Unternehmens umzusehen, Geschäftsverbindungen zu ermitteln und mit Original-Dokumenten Kontoverbindungen so abzuändern, dass Gelder auf Konten der Betrüger gelandet sind (Payment Fraud). In drei Angriffen wurden insgesamt 1,35 Millionen Euro erbeutet. Es hat vier Wochen gedauert, bis der Schaden bemerkt wurde, und eine weitere Woche, bis die Polizei eingeschaltet wurde. Wenn Überweisungen an andere als die bisher gewohnten Bankverbindungen verlangt werden, sollte, so die Experten, zuvor mit dem Geschäftspartner noch zur Verifizierung in Verbindung getreten werden. Verdacht sollte jedenfalls erregen, wenn nicht nur die Kontonummer, sondern sogar die am Anfang der IBAN stehende Landeskennung verändert wurde.

Spoofing. „Sexpressung“ ist eine Form der Erpressung, dass jemand vorgibt, sich auf dem Rechner des Opfers eingenistet und dessen Mail- und Browser-Kontakte, etwa auf Pornoseiten, mitverfolgt zu haben. Es wird mit Veröffentlichung gedroht, sofern nicht Geldbeträge, in der Regel von 1.000 bis 5.000 Euro, in Bitcoins gezahlt würden. Zweifel an der Glaubwürdigkeit der

FOTO: CHINNARACH/STOCK.ADOBE.COM

Vorsicht beim Öffnen von E-Mail-Anhängen: Word-Dateien könnten schädliche Makros enthalten.



Wenn man mit der Maus über die Absenderadresse streicht, sieht man die wahre Adresse, von der die Mail verschickt wurde.

aufgestellten Behauptungen werden dadurch zerstreut, dass als Absender der E-Mail der Empfänger selbst angegeben wird, was den Anschein erweckt, der Angreifer würde sich tatsächlich im System des Angegriffenen befinden. In Wirklichkeit aber kann die Absenderadresse beliebig gestaltet werden (Spoofing). Im Internet können gespoofte Adressen gekauft oder in Auftrag gegeben werden. Erst ein „Mouse over", indem man mit der Maus über die Absenderadresse streicht, offenbart jene Adresse, von der aus die E-Mail abgesendet wurde. Dazu ist wichtig, den Aufbau einer IP-Adresse zu kennen, und die Referenten lieferten dazu auch das nötige Rüstzeug, wobei im Folgenden auf die in der Präsentation gezeigten Beispiele zurückgegriffen wird.

Bei der Web-Adresse *https://primenow.amazon.de* bezeichnet *https* die Sicherheitsstufe des Übertragungsprotokolls („s" für verschlüsselt, im Gegensatz zu *http)* und *primenow* eine Unterkategorie der eigentlichen, weltweit einzigartigen Domain (von den Referenten als „Wer-Bereich" bezeichnet) *amazon.de*. An diese können sich, durch Schrägstriche (Slashes) getrennt, noch beliebig viele weitere Ordner anschließen.

Als Faustregel haben die Referenten den Seminarteilnehmern mitgegeben, dass alles, was zwischen dem zweifachen und dem einfachen Schrägstrich steht, die Absenderadresse betrifft, und davon – als Domain entscheidend – der letzte Teil vor dem einfachen Schrägstrich. Dieser „Wer-Bereich" ist bei der Adresse *http://microsoft.com.account-settings.com/* nicht *microsoft.com,* sondern account-settings.com. Eine angeblich von *Paypal* stammende E-Mail mit der Absender-Adresse *service@paypal.sicherheit.de,* mit der die Zustimmung zu einer Änderung der AGBs durch Anklicken des Buttons bestätigt werden soll, stammt nicht von Paypal, sondern von der Domain sicherheit.de, und ist somit ein Fake. Ebenso die Website *http://paypal.sicherheit.de/details,* über die angeblich Näheres erfahren werden kann.

Täuschungen können auch dadurch erfolgen, dass Absenderadressen auf den ersten Blick bekannt erscheinen, in Wahrheit aber durch andere Zeichen oder Auslassungen verfälscht sind (Buchstabendreher). Von den Adressen *@amzon.com, @arnazon.com* oder *@amaz0n.com* einlangende Mails oder Zahlungsaufforderungen stammen nicht von Amazon, sondern sind Betrügern zuzurechnen.

E-Mail-Anhänge. Die Teilnehmer an dem Seminar konnten über die Chat-Funktion darüber abstimmen, welche Dateiarten von Anhängen zu E-Mails sie als am gefährlichsten erachten würden. Zur Auswahl standen, und hier bereits in die richtige Reihenfolge gebracht, Dateien mit den Endungen *.exe, .doc, .pdf* und *.txt*.

Exe-Dateien werden beim Anklicken direkt ausgeführt, sind also als Anhang am gefährlichsten und kommen in der Praxis nur in Ausnahmefällen vor, über die man sich zuvor vergewissern sollte.

Word-Dateien könnten schädliche Makros enthalten. Der Aktivierung der Makro-Funktion muss zwar zugestimmt werden, was aber schnell mal geschehen sein kann. Geschäftliche Ankündigungen werden üblicherweise nicht im *Word*-Format, sondern als *Pdf* versendet. Ein unübliches *Word*-Dokument sollte daher zur Vorsicht veranlassen.

Pdf-Dateien sind, von in ihnen enthaltenen Links abgesehen, an sich zwar sicher (weshalb Unternehmen empfohlen wird, etwa Lebensläufe von Jobsuchenden im *Pdf*-Format zu verlangen), doch liegt die Gefahr darin, dass nicht die neueste, sondern ältere Versionen des *Acrobat Readers* verwendet werden, die Sicherheitslücken enthalten können.

Textdateien sind die ungefährlichsten, doch muss man bei diesen auf versteckte Endungen (Scripts; etwa *.txt.vbs)* achten. Die letzte Endung *(.vbs)* ist die ausschlaggebende.

In komprimierten Dateianhängen (Endung *.zip)* kann alles Mögliche an Schadprogrammen enthalten sein, weshalb die Experten raten, solche Dateien zur näheren Abklärung auf einem separaten Rechner zu öffnen.

Empfehlungen. Man sollte sich zur Regel machen, bei E-Mails genau auf den (vermeintlichen) Absender sowie auf die Art der Dateianhänge zu achten und nicht unbedacht auf Links oder Buttons zu klicken. In Zweifelsfällen sollte auf der Grundlage vorhandener Daten beim vermeintlichen Absender rückgefragt werden.

Wurden früher Passwörter in der Länge von etwa 8 Zeichen als ausreichend erachtet, gelten heutzutage in Anbetracht der gestiegenen Rechnerleistung 16 Zeichen als Minimum. Je länger, umso besser. Die Passwörter sollten Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen enthalten. Wichtig auch: Für jede Anwendung sollte ein eigenes Passwort verwendet werden, damit im Fall einer Kompromittierung eines Passwortes zu einem Dienst nicht alle anderen auch betroffen werden.

Kurt Hickisch

FOTOS: 4ZEVAR – STOCK.ADOBE.COM, SIEGBERT LATTACHER