Ansprechpartner

Bei Verdacht auf einen IT-Sicherheitsvorfall kontaktieren Sie bitte umgehend die IT-Hotline unter der Telefonnummer 030 227-117.

Die IT-Hotline steht Ihnen auch bei Fragen zu Dienstleistungen der Unterabteilung IT zur IT-Sicherheit (z. B. E-Mail-Verschlüsselung) gerne zur Verfügung und leitet Ihre Anfragen ggf. an die zuständigen Stellen weiter.

Weiterführende Informationen

Weiterführende Informationen zum Thema Informationssicherheit finden Sie im Intranet unter: https://sicher-vernetzt.bundestag.btg

Oder im Internet beispielsweise auf folgenden Seiten:
https://www.bsi.bund.de
https://www.bsi-fuer-buerger.de
https://www.buerger-cert.de

Besuchen Sie die Basisschulung zur Informationssicherheit am Arbeitsplatz im IT-Schulungszentrum. Informationen finden Sie unter: https://sicher-vernetzt.bundestag.btg/Schulungen/schulungen.php

Impressum

Herausgeber: Deutscher Bundestag, Referat IT 2
Neue Informationssysteme, IT-Beschaffung, Rechtsfragen der Informationsverarbeitung, Schulung und Benutzer-Service
Layout: Deutscher Bundestag, Referat ZT 5
Zentrale Bedarfsdeckung und Logistik
Bundestagsadler: Urheber Prof. Ludwig Gies, Bearbeitung 2008 büro uebele
Grafik: Deutscher Bundestag / Detlef Surrey
Druck: H. Heenemann GmbH & Co. KG, Berlin

Stand: Dezember 2018;

Spam, Phishing und Co. – was ist das eigentlich?

Unter dem Begriff *Spam* werden generell unerwünschte E-Mails zusammengefasst. Diese enthalten meist Werbung, beispielsweise für Arzneimittel oder Kredite, und werden ungezielt an eine Vielzahl von Empfängern versandt. Die E-Mail-Adressen können dabei von Adresshändlern stammen oder durch spezielle Programme im Internet gesammelt worden sein.

Mittels *Phishing-E-Mails* versuchen Betrüger, Zugriff auf vertrauliche Daten wie Benutzernamen, Passwörter, Kreditkartennummern und TANs zu erlangen. Phishing ist ein Kunstwort, bestehend aus „Passwort“ und „Fishing“ – frei übersetzt etwa „Fischen nach Passwörtern“. Dazu werden die Empfänger über einen in der E-Mail enthaltenen Link auf eine täuschend echt aussehende – aber gefälschte – Webseite gelockt und dazu gebracht, dort ihre Zugangsdaten einzugeben. Herkömmliche Phishing-Attacken besitzen, verglichen mit der Anzahl der gesendeten E-Mails, nur eine geringe Erfolgsquote, da sie undifferenziert an möglichst viele Empfänger geschickt werden.

Dahingegen zielen *Spear-Phishing-Attacken* auf eine bestimmte Zielgruppe (oder auch nur eine bestimmte Person) ab und sind auf diese zugeschnitten. Dieses Vorgehen verspricht einen größeren Erfolg und wird seltener aufgedeckt. Die Angreifer nutzen dabei häufig Methoden des Social Engineering, um verlässliche Informationen über die Person bzw. Zielgruppe zu erhalten. Derartige E-Mails zu enttarnen, kann besonders schwierig sein: Oftmals stammen diese von einem vermeintlich bekannten Absender und lassen von Betreff und Inhalt her vermuten, dass es sich um eine legitime E-Mail handelt. Derartige Informationen kann der Angreifer beispielsweise von bereits erfolgreich infizierten Computern abgegriffen haben.

E-Mails, die im Anhang versteckt ein Schadprogramm (z. B. ein „Trojaner“) enthalten, werden als *Malspam* bezeichnet. Auch Malspam kann entweder mittels Gießkannenprinzip oder gezielt versandt werden. Ziel des Angreifers ist es, einen fremden PC oder Laptop mit einer Schadsoftware zu infizieren. Diese kann beispielsweise Angriffsmodule zum Ausspähen oder Verschlüsseln von Daten aus dem Internet herunterladen. Öffnet der E-Mail-Empfänger einen derart präparierten Anhang, wird die Schadsoftware ausgeführt. Besonders arglistig ist, dass der Empfänger unbewusst dazu gebracht wird, bestehende Sicherheitsmechanismen zu umgehen, indem er beispielsweise Makros in Word-Dokumenten oder alle Funktionen in PDF-Dateien aktiviert. Handelt es sich um eine bekannte Schadsoftware, wird diese von der Antivirensoftware unschädlich gemacht. Neue oder extra für diesen Angriff entwickelte Schadsoftware wird jedoch nicht sofort erkannt und kann unbemerkt ihr Unwesen auf dem Rechner treiben.

Deutscher Bundestag

IT-Sicherheitskampagne – Sicher vernetzt im Parlament

Tipps zum Schutz vor Spam, Phishing und Co.

Alle Jahre wieder…

Weihnachtsgrüße werden heutzutage oftmals per E-Mail versandt und Weihnachtsgeschenke beim Online-Händler bestellt. Daher ist es nicht verwunderlich, dass die Weihnachtszeit auch für den Versand von Spam-, Phishing- und Malspam-E-Mails beliebt ist.

Ob Spam, Phishing oder Malspam: Unerwünschte E-Mails können einen immensen Schaden anrichten. Wichtig ist daher, dass Sie folgende Tipps – nicht nur zur Weihnachtszeit – beherzigen:
Prüfen Sie Absender und Inhalt einer E-Mail immer auf Plausibilität.
Bei Zweifeln an der Plausibilität:

- Öffnen Sie beigefügte Anhänge nicht.
- Klicken Sie nicht auf enthaltene Links.
- Antworten Sie nicht auf die E-Mail.
- Lassen Sie die E-Mail nicht im HTML-Format anzeigen.
- Löschen Sie die E-Mail umgehend – auch im Ordner „Gelöschte Elemente“!

Sollten Sie versehentlich einen Anhang geöffnet oder einen Link aufgerufen haben, kontaktieren Sie bitte die IT-Hotline unter der 030 227-117. Der IT-Support wird prüfen, ob Ihr Parlakom-PC oder -Laptop mit einer Schadsoftware infiziert sein könnte. Ggf. erfolgt eine Neuinstallation des Gerätes. Denken Sie auch daran, in diesem Fall ggf. eingegebene Zugangsdaten umgehend zu ändern!

So erkennen Sie Spam, Phishing und Co.

Bevor Sie einen E-Mail-Anhang öffnen oder einen Link anklicken, sollten Sie E-Mails immer auf Plausibilität prüfen. Folgende Fragen können Ihnen dabei helfen, gefährliche E-Mails zu enttarnen:

Erwarten Sie die E-Mail?

Oftmals können Phishing-E-Mails oder Malspam auf den ersten Blick als solche erkannt werden, wenn Ihnen beispielsweise eine angebliche Rechnung oder Mahnung eines Unternehmens zugestellt wird, bei dem Sie kein Kunde sind. Wenn Sie kein Paket erwarten, sind Sendungsbenachrichtigungen unwahrscheinlich. Behördliche oder anwaltliche Schreiben erfordern häufig eine gerichtsfeste Schriftform, also die Zustellung per Brief.

Kennen Sie den Absender?

Absenderadressen von E-Mails können leicht gefälscht werden. Kriminelle, die Schadsoftware auf Ihren PC bringen wollen, verstecken sich gerne hinter fremden E-Mail-Adressen. Daher sollten Sie genau prüfen, ob die E-Mail-Adresse vertrauenswürdig erscheint. Lassen Sie sich dabei nicht vom Anzeigenamen täuschen, denn auch dieser kann falsch sein. Gewissheit über die Echtheit einer Absenderadresse kann eine digitale Signatur liefern. Ist diese nicht vorhanden, fragen Sie im Zweifelsfall telefonisch beim Absender nach, ob die E-Mail von ihm versendet wurde.

Durch einen Blick in den E-Mail-Header / die Internetkopfzeile können Sie ebenfalls nachschauen, von wem die E-Mail stammt. Hierbei kann Ihnen die IT-Hotline behilflich sein.

Werden Sie persönlich angesprochen?

Eine unpersönliche Anrede (z. B. „Sehr geehrter Kunde“) kann ein Zeichen für eine Phishing-E-Mail sein. Ein Freund oder Geschäftspartner würde Sie sehr wahrscheinlich direkt mit Ihrem Namen ansprechen.
Aber: Auch der persönlichen Anrede können Sie nicht ungeprüft vertrauen.

Sollen Sie vertrauliche Daten eingeben (z. B. Benutzername, Passwort, TAN-Nummer)?

Quasi als „besonderes Serviceangebot“ enthalten gefährliche E-Mails häufig einen Link/Button, über den Sie angeblich direkt auf die Internetseite des Online-Händlers oder Ihrer Bank gelangen. Klicken Sie nicht auf Links in zweifelhaften E-Mails – diese führen vermutlich zu gefälschten Webseiten! Von dort kann binnen Sekunden und ohne Ihr Wissen eine Schadsoftware heruntergeladen und installiert werden. Tippen Sie stattdessen die Internetadresse des Online-Händlers oder Ihrer Bank in den Internetbrowser ein, melden sich an und prüfen, ob Meldungen für Sie vorliegen. Im Zweifelsfall fragen Sie telefonisch nach.

Haben Sie den Anhang/Link angefordert?

Oftmals enthalten schadhafte E-Mails als Anhang eine angebliche Rechnung, Mahnung oder Bestellbestätigung mit gängigen Dateiendungen wie .doc, .docx, .pdf oder .zip. Im beruflichen Kontext könnten stattdessen geschäftliche Schreiben, Protokolle, Einladungen oder Bewerbungsunterlagen vorgetäuscht werden.
Als Alternative zum E-Mail-Anhang werden derartige Dokumente immer häufiger über einen Link zum Download bereitgestellt. Allen gemeinsam ist: Es handelt sich um E-Mails, über die Schadsoftware auf PC, Laptop, Tablet-PC oder Smartphone eingeschleust werden soll.

Prüfen Sie auch hier die Plausibilität: Passt der Absender zum Anhang? Haben Sie den Anhang bzw. Link erwartet? Würde Ihnen der Absender wirklich einen Link zum Abruf von Sitzungsunterlagen aus dem Internet zusenden?

Öffnen Sie Anhänge bzw. Links in E-Mails nur, wenn Sie sich sicher sind, dass es sich um eine legitime E-Mail handelt. Auch hier kann ein Anruf beim angeblichen Absender Gewissheit bringen.

Weist die E-Mail viele Rechtschreib-, Grammatik- oder Zeichensetzungsfehler auf?

Auch schlechtes Deutsch, Rechtschreib-, Grammatik- und Zeichensetzungsfehler können ein Indiz für eine Phishing-E-Mail sein, denn derartige E-Mails werden oftmals maschinell ins Deutsche übersetzt. Jedoch werden die Texte schadhafter E-Mails immer besser.

Passen Sprache und Anrede zum Absender?

Erhalten Sie eine E-Mail eines angeblichen Geschäftspartners auf Englisch, obwohl Sie bisher nur Deutsch miteinander kommuniziert haben? Abweichungen in der verwendeten Sprache (z. B. Englisch statt Deutsch) oder in der Anredeform (z. B. duzen statt siezen) können ebenfalls auf eine gefälschte E-Mail hindeuten.

Achten Sie auf Ihr Bauchgefühl!

Aber Vorsicht: Es gibt auch professionell und (nahezu) fehlerfrei gestaltete E-Mails. Auch wenn eine E-Mail von einem vermeintlich bekannten Absender stammt, die Absenderangaben am Ende der E-Mail korrekt erscheinen, Betreff und Inhalt plausibel klingen oder Sie einen vergleichbaren Anhang erwarten, kann es sich um eine gefälschte E-Mail handeln.

Vertrauen Sie daher auf Ihr Bauchgefühl!
Sollten Sie an der Echtheit einer E-Mail zweifeln, kontaktieren den Absender der E-Mail oder die IT-Hotline unter der 030 227-117.