Gefahren durch E-Mail Inhalte, Anlagen und Links uneingeschränkt hoch

Die „Angriffe“ über das Medium E-Mail nehmen ständig zu. Ebenso steigt die „Qualität“ und „Professionalität“.

Warum sind gefährliche E-Mails so schwer zu erkennen?

1. Auch wenn der Name und/oder die E-Mail-Adresse des Absenders Ihnen bekannt ist, kann sich trotzdem eine gefährliche E-Mail dahinter verstecken! Das gilt auch für E-Mails von Personen aus dem eigenen Unternehmen.
   Warum ist das so?
   - Die E-Mail kann im Namen des Absenders abgesendet worden sein – denken Sie an den Enkeltrick – und das E-Mail Sicherheitssystem hat den Betrug nicht erkannt.
   - Das E-Mail-Konto des Absenders wurde gehackt und die E-Mail wurde „wirklich“ aus dem Postfach des Absenders ohne sein Wissen versendet.
   - Der Mailserver des Absenders wurde gehackt und die E-Mail wurde „wirklich“ vom Mailserver im Namen des Absenders ohne sein Wissen versendet.
2. Der Inhalt der E-Mail ist auf Sie persönlich oder auf Ihr Unternehmen bzw. Branche zugeschnitten. Es ist extrem schwer zu erkennen, dass es sich um eine Betrugs E-Mail handelt, da Sie eventuell direkt namentlich angesprochen werden oder der Inhalt auf Ihren Tätigkeitsbereich abzielt, wie z.B. eine als Anfrage getarnte E-Mail an einen Vertriebsmitarbeiter bzw. eine als Angebot getarnte E-Mail an einen Einkaufsmitarbeiter.

Nachfolgend finden Sie Informationen und Empfehlungen zum „sichereren“ Umgang beim Empfang von E-Mails. 100%ige Sicherheit gibt es nicht.

1. Folgen Sie der 3-Sekunden Empfehlung beim Empfang von E-Mails des Bundesministeriums für Sicherheit in der Informationstechnik BSI:
   Mit einem 3-Sekunden-Sicherheits-Check können die Risiken bereits gemindert werden. Absender, Betreff und Anhang sind hierbei drei kritische Punkte, die vor dem Öffnen jeder E-Mail bedacht werden sollten. Ist der Absender bekannt? Ist der Betreff sinnvoll? Wird ein Anhang von diesem Absender erwartet? In Kombination liefern diese Fragen einen guten Anhaltspunkt, um zu entscheiden, ob die E-Mail als vertrauenswürdig einzustufen ist. In vielen Spam-Mails ist der Betreff bewusst vage formuliert, wie "Ihre Rechnung", "Mahnung" oder "Dringende Nachricht". Hier gilt es besonders kritisch zu hinterfragen, ob eine Nachricht vom jeweiligen Absender sinnig erscheint, insbesondere, wenn Mail-Anhänge beigefügt sind. Erhalten Sie beispielsweise eine E-Mail mit dem Betreff „Rechnung“ von einem Online-Shop, bei

GCT Gesellschaft für Computer-Technologie mbH
Hausanschrift Im Atzelnest 3 · 61352 Bad Homburg
Telefon 06172 9486-0 · Telefax 06172 9486-94
Mail hallo@gct.de · Web www.gct.de
Twitter @GCT_BadHomburg · Facebook facebook.com/gct.it

Autor: Udo Janßen
Erstellt am: 14.12.2019
Revision am: Erstausgabe

Gefahren durch E-Mail Inhalte, Anlagen und Links uneingeschränkt hoch

dem Sie registriert sind, ohne dass Sie eine Bestellung erwarten, könnte dies ein Hinweis für eine Spam-Mail sein. Hinterfragen Sie jede E-Mail: Ergibt die Überprüfung der drei Checkpunkte Absender, Betreff, Anhang insgesamt kein stimmiges Bild, rät das BSI E-Mails noch vor dem Öffnen zu löschen. Im Zweifelsfall sollten Sie vor dem Öffnen persönlich beim Absender nachfragen, ob er eine E-Mail geschickt hat.
(Quelle: Website des Bundesamts für Sicherheit in der Informationstechnik)

2. Trauen Sie Links in E-Mails nur, wenn Sie Punkt 1 beachtet haben und der Klick auf den Link wirklich für die Bearbeitung der E-Mail Relevanz hat.
3. Links in E-Mails können „versteckt“ sein. Das Ziel ist ohne genaueres Hinsehen nicht zu erkennen. Nachfolgend ein Beispiel – bitte nicht KLICKEN, nur mit der Maus über den Link fahren, dann erscheint das Ziel, dass hinter dem Link liegt:
   a. fahren Sie mit der Maus ohne zu klicken auf den Link BSI-Artikel
   b. fahren Sie mit der Maus ohne zu klicken auf den Link BSI-Artikel
   Sie sehen den Unterschied?
   Bei a. sehen Sie den korrekten Link zum BSI-Artikel. Bei b. liegt ein Phantasie Link dahinter, der auf eine Website mit Schadcode führen könnte.
4. Leiten Sie E-Mails nicht an andere Empfänger innerhalb oder außerhalb Ihres Unternehmens weiter, die dem 3-Sekunden-Sicherheits-Check nicht standhalten.

Seien Sie IMMER wachsam und klicken Sie nicht sofort auf Links in einer E-Mail oder öffnen Sie nicht direkt E-Mail Anlagen!

Udo Janßen ist seit 1990 bei GCT und seit 2001 als geschäftsführender Gesellschafter für die Technik verantwortlich. Er hat bei zahlreichen Unternehmen Netzwerk- und Securityinfrastrukturen aufgebaut und ist von Herstellern wie u.a. SonicWALL, Microsoft, VMware, Kemp als Administrator zertifiziert worden.

GCT ist seit 1989 Ihr professioneller IT-Dienstleister im Rhein-Main-Gebiet mit Sitz in Bad Homburg v.d.H. Als klassisches IT-Systemhaus betreuen wir Ihre IT im eigenen Haus, als Outsourcer bringen wir Ihre IT in eine private Cloud im GCT Rechenzentrum in Frankfurt am Main oder in die public Cloud namhafter Anbieter und als Managed Service Anbieter liefern wir Ihnen Anwendungen und Security „as a Service“.

GCT Gesellschaft für Computer-Technologie mbH
Hausanschrift Im Atzelnest 3 · 61352 Bad Homburg
Telefon 06172 9486-0 · Telefax 06172 9486-94
Mail hallo@gct.de · Web www.gct.de
Twitter @GCT_BadHomburg · Facebook facebook.com/gct.it

Autor: Udo Janßen
Erstellt am: 14.12.2019
Revision am: Erstausgabe