Weshalb sind E-Mail Speerfischer-Angriffe (Spear-Phishing) so gefährlich

Was unterscheidet E-Mail Speerfischer-Angriffe (Spear-Phishing) von herkömmlichen Phishing-Emails?

Zur Erklärung: Was steckt hinter dem Begriff Phishing-Email?

> Phishing wird vom englischen Wort für „fischen/angeln“ also fishing abgeleitet. Bei dieser Methode geht es den Angreifern vornehmlich darum, Zugangsdaten wie Benutzernamen und Passwörter bzw. allgemein „digitale Identitäten“ zu erlangen und diese in der Regel für kriminelle Handlungen zum Schaden des betroffenen Benutzers zu verwenden. Häufig werden auch ergaunerte Adressen aus dem Adressbuch des Betroffenen für weitere Angriffe genutzt.
> Beim Phishing allgemein geht der Angreifer in der Regel nach dem Prinzip der massenhaften Versendung von Phishing E-Mails vor. Trotz der mittlerweile verbreiteten Information über die Gefahr solcher Attacken und auch allgemeiner Schutzmaßnahmen wie Spam-/Phising-Filter, tappen immer wieder einzelne Benutzer in die Falle.

Kommen wir nun zum Spear-Phishing (also dem gezielten Fischen von Informationen auf einen einzelnen bzw. wenige Zielbenutzer mit einem direkten „Speer“-Angriff)

> Beim Spear-Phishing geht der Angreifer nun gezielt auf einzelne Opfer los, anstatt wie beim normalen Phishing tausende Adressaten anzuschreiben. Sinnbildlich wird mit dem Speer ein einzelner Fisch angegriffen.
> In der Regel wird der Angriff auf einzelne oder wenige Adressaten ausgeführt, über die der Angreifer im Vorfeld Informationen eingeholt hat. Häufig sieht man Angriffe im Bereich des Personalmanagements, wo auf bestehende Personalanzeigen gezielte Bewerbungs-E-Mails mit gefährlichem Inhalt (Anlagen oder Links) gesendet werden.
> Lassen Sie Ihrer Phantasie freien Lauf. Sie werden in Ihrem beruflichen und privaten Interessen Umfeld selber viele Angriffspunkte finden, bei denen Sie „angreifbar“ sind.

Wie soll man sich nun verhalten?

> Technische Schutzmaßnahmen wie Spam- und Phishing Filter (die bei Unternehmen und auch in den meisten Online Postfächern eingesetzt werden)

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

Weshalb sind E-Mail Speerfischer-Angriffe (Spear-Phishing) so gefährlich

sind obligatorisch. Ohne solch „vorgeschalteten“ Schutzmechanismus vor seinem Postfach geht man meistens nach ein paar Jahren in Spam E-Mails unter.
Zusätzlich ist auch ein aktueller Virenscanner (aktuell von Programmversion als auch der Virendefinition) obligatorisch, um überhaupt die Chance einer Erkennung und Abwehr zu erhalten, falls man doch einmal unaufmerksam war und eine Datei oder einen Link in einer solchen E-Mail angeklickt hat.
Achten Sie auf Warn-Meldungen und Hinweise Ihrer E-Mail-Programme, Virenscanner und auch Browser. Viele der aktuellen Programme besitzen Erkennungsmechanismen für gefährliche Inhalte. Ignorieren Sie diese Hinweise nicht.
Mittlerweile lassen sich die gefährlichen E-Mails nicht mehr so leicht an Rechtschreibfehlern und schlechter Wortwahl erkennen. Die Angreifer sind da weitestgehend professionell und lassen sich nicht mehr so leicht identifizieren.
Weiterhin gelten die Empfehlungen aus meiner GCT Empfehlung 201912A, die Sie in unserem Blog https://blog.gct.de finden können.

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“.