IT-Sicherheitsinformationen

Betrügerische E-Mail-Nachrichten (sogenanntes „Phishing“) zählen zu den gegenwärtig gefährlichsten Bedrohungen der IT-Sicherheit. Dabei wird versucht, an Anmeldedaten zu gelangen oder Schadsoftware auf dem Computer zu installieren. Im Frühjahr 2021 hat es auch zwei gegen die PH Ludwigsburg gerichtete Angriffsversuche per Phishing gegeben.

Ausführliche Informationen finden Sie im Dokument „Phishing-Prävention_V20.pdf“, das ebenfalls auf der IT-Sicherheitsseite des MIT steht. Nachfolgend die wichtigsten Ratschläge kurz zusammengefasst:

Prüffragen bei verdächtigen E-Mail-Nachrichten

- Sind der Absendername und E-Mail-Adresse vollständig und korrekt angegeben?
- Ist der Inhalt glaubwürdig und bezieht er sich auf Vorgänge, die normalerweise in Ihrem Aufgabenbereich liegen?
- Ist die Nachricht in Stil und Sprache regulär formuliert? (ordentliche Anrede, präzise Rechtschreibung, bekannte Grußformel und Name, vollständige Signatur)
- Wahrt die Nachricht die gebotene Distanz oder werden Sie zu unmittelbarem Handeln gedrängt? Beispiel: „Wenn Sie nicht bis morgen X machen, wird Ihr Konto gesperrt.“

Grundsätzlich:

- Bei allen externen Mails, die Links und Anhänge enthalten, ist besondere Vorsicht geboten. Hier müssen Absenderfeld und Link überprüft werden. Näheres dazu im bereits erwähnten angehängten Dokument.
- Alle Mitteilungen zur IT (z.B. Ankündigungen von Wartungsmaßnahmen) stammen ausschließlich von Angehörigen des MIT (Zentrum für Medien und Informationstechnologie) und werden namentlich unterzeichnet. Mitteilungen angeblich direkt von Microsoft oder dergleichen, sowie solche, die etwa mit „Ihre Administratoren“ unterzeichnet wurden, sind Betrug.
- Geben Sie keinesfalls auf einer (durch einen Link aufgerufenen) Webseite Ihre Anmeldedaten (Benutzername und Passwort) ein!
- Antworten Sie nicht auf verdächtige oder sonstwie merkwürdige E-Mails, auch wenn diese keine Links oder Anhänge enthalten. Es wird eventuell versucht, die angeschriebene Adresse zu verifizieren. Eine als real existierend bestätigte Adresse ist potentielles Ziel für spätere Angriffe.
- Empfehlung: Einmal im Monat den Virenscanner TrendMicro (im Startmenü unter „Trendmicro Apex One Security Agent – Security Agent“ zu einem Gesamtscan des gesamten PCs aufrufen.

Hilfreich zu wissen:

- E-Mails, die von Absendern außerhalb der Hochschule stammen, sind im Betreff mit [extern] gekennzeichnet. Wenn eine E- Mail, die mit dem Namen eines Hochschulangehörigen unterzeichnet ist, die [extern]-Markierung enthält, ist dies verdächtig.
- Unaufgeforderte E-Mails von populären Institutionen und Firmen (Microsoft, Post, und DHL, Deutsche Bahn, Amazon und Ebay, Paypal, Sparkasse, Volksbank, generell alle Banken, usw.) sind per se verdächtig, weil deren Kommunikation in großem Umfang von Cyberkriminellen gefälscht wird.
- Leiten Sie im Zweifelsfall die E-Mail-Nachricht an die Adresse „virusverdacht@ph-ludwigsburg.de“ weiter. Das MIT-Team prüft die Nachricht und gibt Ihnen Rückmeldung.

Tragen Sie durch sorgfältige Gestaltung Ihrer eigenen E-Mails zur Sicherheit bei:

- Verwenden Sie in Ihren dienstlichen Aufgaben ausschließlich das E-Mail-System der Hochschule (dienstliche E-Mail-Adresse). Bei außerhochschulischen E-Mail-Absendern (z.B. privates E-Mail-Konto) besteht das Risiko, dass diese Mails aufgrund von (irrtümlich angenommenen) Phishing-Merkmalen oder wegen der ungewöhnlichen Adressangaben durch technische Filter geblockt werden.
- Unterzeichnen Sie jede Nachricht mit Ihrem Namen und einer vollständigen Signatur entsprechend des PHL-Standards (vgl. Signatur unten).
- Kennzeichnen Sie E-Mail-Nachrichten, wenn diese von anderen Personen formuliert wurden (z.B. Vorgesetzte), immer auch mit Ihrem Namen, z.B. „(im Auftrag, IHR NAME)".
- Geben Sie Internetadressen (URL) vollständig sichtbar an, nicht versteckt in einem verlinkten Text (Bsp.: „Klicken Sie hier").

Weitere sicherheitsrelevante Hinweise:

- Sie tragen die Verantwortung, dass keine unbefugten Personen Zugriff auf Ihr Gerät und die damit verbundenen Daten und IT-Dienste erhalten. Insbesondere in Räumen mit hohem Publikumsverkehr, im Home-Office und beim mobilen Einsatz unterwegs: Sperren Sie bei jedem Weggang von Ihrem Rechner den Bildschirm.
- Lassen Sie keine Dokumente im Drucker oder in Seminarräumen liegen.
- Dienstliche Unterlagen sind im Home-Office in verschlossenen Behältnissen, gesichert vor dem Zugriff Dritter, aufzubewahren.
- Nicht mehr benötigte dienstliche Unterlagen werden auf dem Campus in einem Container oder Schredder entsorgt.
- Wenn Sie – auch nur gelegentlich - private Rechner für die die Arbeit an der Hochschule verwenden, muss auf diesen ein leistungsfähiger Virenscanner installiert sein. Der an der PHL eingesetzte Virenscanner TrendMicro kann auch privat genutzt werden. Dieser ist sowohl für Mac als auch für Windows verfügbar und kann im Downloadzentrum unter „Kategorien > Software" heruntergeladen werden.
- Das Kapitel „IT—Sicherheit" informiert fortlaufend über Sicherheitshemen. Sie finden dieses Kapitel unter:
  Hochschule > Einrichtungen > Zentrum für Medien und Informationstechnologie (MIT) > IT-Sicherheit
- Auf der Lernplattform Moodle finden Sie unter „Meine Startseite > Meine Kurse > Verschiedenes > Zentrum für Medien und Informationstechnologie (MIT) > IT-Sicherheit eine Präsentation zur IT-Sicherheit sowie zwei Sicherheitstests als Multiple Choice Quiz.

Updates

Updates müssen immer aus sicheren Quellen, im allgemeinen vom Originalhersteller, bezogen werden. Die nicht dauerhaft überprüften Links auf den Webseiten von PC-Zeitschriften oder von Foren sind oft manipuliert und führen zu betrügerischen Seiten, die Anmeldedaten abgreifen oder statt des Updates bzw. zusätzlich zum Update Malware installieren. Daher bitte auch genau kontrollieren, ob man sich wirklich auf einer Seite des Herstellers/Diensteanbieters befindet.

Links auf Webseiten

Generell muß die Gültigkeit einer verlinkten Webseite aufmerksam geprüft werden, denn ein Link kann zu einer gefaketen Seite führen, deren Adresse und Gestaltung der echten täuschend ähnlich sieht. Deswegen empfiehlt es sich, öfters kontaktierte Webseiten unter „Favoriten" zu speichern und von dort aus aufzurufen. Auch bei selten oder bisher noch nie kontaktierten Webseiten sollte nicht

der Link in der Mail verwendet werden. Stattdessen sollte man die Zieladresse über den Browser suchen und starten.

Vor dem Klick auf einen Link und vor allem vor dem Klick auf Schalter oder in Eingabefelder der verlinkten Webseite muß immer überlegt werden, ob der Link einen seriösen Eindruck macht. Auch wenn der Link von einer nachweislich vertrauenswürdigen Person zugeschickt wurde, kann er trotzdem schädlich sein, weil der Absender dem betrügerischen Link vertraut hat und diesen daher in bester Absicht weitergeleitet hat. Auch in Webkonferenzen mit einem großen Teilnehmerkreis muß man bei Links, die ins Chatfenster gestellt wurden, vorsichtig sein. Es kann sich ein Böswilliger eingeschlichen haben, der bewußt schädliche Links verbreiten will.

Passwörter

Länge: Das wichtigste Kriterium eines sicheren Paßworts ist die Länge. Allein schon eine Stelle mehr vervielfacht die Suchzeit, bis durch automatisiertes Ausprobieren die Lösung gefunden wird. 12 Stellen sind gut.
Komplexität: Im Wörterbuch auffindbare Wörter sind ganz schnell geknackt. Daher sollte man willkürliche, nicht sinntragende Kombinationen aus Groß- und Kleinbuchstuben, Sonderzeichen und Zahlen verwenden. Dies geht am einfachsten, wenn man das Kennwort aus den ersten Zeichen jeden Wortes eines längeren Satzes zusammensetzt.
Ich wurde am 17.5.1999 geboren und heiße Sabine Testuser
Iwa17.5.1999guhST

Verteilung von Dateien

[am Rande: Moodle ist zur Verteilung von Dateien angelegt – aber nur innerhalb eines Kurses. Für Verteilung an Personen außerhalb eines Kurses ist es ungeeignet.]
Da Mailkonten einerseits gehackt werden können und andererseits deren Speicherkapazität beschränkt ist, sollten vertrauliche oder große Dateien nicht per Mail verteilt werden. Alternativen sind
1. bwSync&Share: Das ist ein Clouddienst für baden-württembergische Hochschulen und eignet sich daher auch für den Datenaustausch mit anderen Hochschulen.
Hier die Startseite:
https://bwsyncandshare.kit.edu/apps/user_saml/saml/selectUserBackEnd?redirectUrl=
Unter dieser Adresse auf der MIT-Homepage finden sie das offizielle Nutzerhandbuch und Lernvideos vom E-Learning-Team der PH:
https://www.ph-ludwigsburg.de/hochschule/einrichtungen/mit/themen-dienste/bwsyncshare
2. Abteilungs- und Projektverzeichnisse
Wenn Dokumente doch per Mail verschickt werden müssen, empfiehlt es sich, diese ins pdf-Format umzuwandeln, was auch den Vorteil bietet, dass der Inhalt nicht vom Empfänger verändert werden kann.
Gefährliche Dateiformate, welche die Ausführung von Befehlen ermöglichen, wie .exe, .com, .bat, .cmd usw., sowie Officedateien mit Makros (docxm, xlsxm) werden vom Mailsystem blockiert und können daher nicht per Mail verschickt werden. Will man solche Dateien, sofern sie selbst erstellt wurden oder aus vertrauenswürdiger Quelle stammen, anderen Personen zugänglich machen, so kann man dies über die gerade beschriebenen Austauschplattformen machen.

Social Engineering

Telephonanrufe sind beliebte Methoden, um sich Zugang zu Ihren Rechnern zu verschaffen oder um zu wertvollen Informationen über das Arbeitsumfeld zu gelangen.
Supportanrufe: hier ist zwischen scheinbar internen und externen Anrufern zu unterscheiden. Bei einem Anruf aus der hauseigenen IT, der sich auf eine Störmeldung bezieht, lassen Sie sich, wenn Sie

nicht ganz sicher die Stimme identifizieren, den Namen, die Ticketnummer bzw. das Thema der Störmeldung nennen. Im Zweifelsfall geben Sie Bescheid zurückzurufen. Achtung: die Telephonnummer im Display ist kein verläßliches Indiz. Sie kann genauso gefälscht werden wie eine Mailadresse.
Externe Supportanrufe sind, sofern Sie nicht selbst eine Störung einer Firmenhotline gemeldet haben, IMMER Betrug. Wenn Sie sich im Büro befinden: Kommunikation zu allen IT-Belangen erfolgt ausschließlich über das MIT. Wenn Sie zu Hause sind: Computerfirmen wie Microsoft oder Apple teilen Informationen zu Updates, Sicherheitswarnungen usw. per Mail u. dgl. mit. Sie haben nicht die Zeit und das Personal, um alle Kunden persönlich anzurufen.
Sollte es einem angeblichen Kundendienstler doch gelungen sein, sich auf Ihren Rechner aufzuschalten, beobachten Sie das weitere Vorgehen ganz genau. Wenn eine Software installiert werden soll oder der Bildschirm schwarz wird, brechen Sie den Kontakt sofort ab und schalten den Rechner aus, um Schlimmeres zu verhüten. Melden Sie den Vorfall dem MIT!

Keinen direkten Schaden, wohl aber indirekten kann eine andere Form von Social Engineering anrichten. Dies betrifft Anrufe, die aushorchen und eine Lage ausspionieren wollen. Scheinbar unverfängliche Informationen, die einem so nebenbei entlockt werden, können für einen Angriff ausgenutzt werden. Beispiele: „ja, nach 19 Uhr ist hier niemand mehr da“, „die Sicherheitsfunktion X mußte aus Performancegründen abgeschaltet werden“, „ja, demnächst sollen hier die Rechner getauscht werden“. Die Angreifer geben sich als Angehörige von Marktforschungsunternehmen, der Polizei, Landesbehörden, von Zeitungen und anderen Medien aus.
Unterschätzen Sie niemals die Findigkeit und Professionalität solche Betrüger! Sie haben sich gründlich vorbereitet, wissen wie man Vertrauen aufbaut, und kennen auf alle Fragen und Einwände eine Antwort.

USB-Stick/Präsentationen

Werden zu Präsentationen USB-Sticks mitgebracht, besteht eine gewisse Gefahr, dass der USB-Stick verseucht ist und Schadsoftware verbreiten kann. Daher sollte er vor der Nutzung durch einen Virenscanner kontrolliert werden. Besser ist es, die Powerpointdatei und andere Materialen auf einem Fileserver oder per bwSyncandShare bereitzustellen.