it-safe.at

IT Sicherheitshandbuch

FÜR MITARBEITERINNEN UND MITARBEITER

8. Auflage

WKO
INFORMATION · CONSULTING

it-safe.at ist eine Initiative der Bundessparte Information und Consulting in der WKÖ (BSIC).

IT Sicherheitshandbuch

FÜR MITARBEITERINNEN UND MITARBEITER

8. Auflage

it-safe.at – das IT-Sicherheitsprojekt für KMU

Impressum

Medieninhaber/Verleger:
Wirtschaftskammer Osterreich, Bundessparte Information und Consulting, 1045 Wien,
Wiedner Hauptstraße 63; ic@wko.at, http://wko.at/ic

8. Auflage, Oktober 2017
Für den Inhalt verantwortlich: Friedrich Tuma, Mag. Verena Becker, Mag. Ursula Illibauer
Basislayout: Birgit Altrichter, Michaela Kock – geschmacksache.at
Grafische Umsetzung: www.designag.at
Druck und Herstellungsort: Grasl Druck und Neue Medien GmbH, 2540 Bad Vöslau

INHALT


© Foto Weinwurm

VORWORT

IT-SICHERHEIT GEHT UNS ALLE AN!

Praktisch jedes Unternehmen ist heute mit der elektronischen Verarbeitung und Speicherung von Daten konfrontiert. Die Bandbreite reicht von Kundendaten über die computerunterstützte Buchhaltung bis hin zu Software- oder Grafikunternehmen, die ihre Produkte und Dienstleistungen mit dem Computer erstellen. Viele Unternehmen sind darüber hinaus mit Daten konfrontiert, die keinesfalls in die Hände Dritter fallen dürfen – sei es aus Gründen des Datenschutzes oder weil es sich um vertrauliche Unternehmensdaten zu neuen Produkten, Marktstudien oder Forschungsergebnissen handelt.

Datensicherheit im Allgemeinen und speziell IT-Sicherheit sind daher unverzichtbar für den Unternehmenserfolg. Unternehmensdaten müssen bestmöglich geschützt werden. Dies gilt sowohl für den Versuch, diese Daten auszuspionieren, als auch für die Gefahr des Datenverlustes durch technische Gebrechen.

AUCH SIE ALS MITARBEITERINNEN UND MITARBEITER SIND GEFORDERT!

Gerade in kleineren Unternehmen sind jede einzelne Mitarbeiterin und jeder einzelne Mitarbeiter gefordert. Deswegen tragen auch Sie zur Sicherheit und somit zum wirtschaftlichen Erfolg Ihres Unternehmens entscheidend bei! Bereits das einmalige Anklicken eines bösartigen Links kann dazu führen, dass das gesamte Netzwerk im Unternehmen mit Malware infiziert wird.

Das vorliegende Handbuch liegt nun in der 8. Auflage vor und soll für Sie eine Hilfestellung zu den wichtigsten Fragen der IT-Sicherheit sein. Gleichzeitig ist es eine Handlungsaufforderung: Sprechen Sie mit den IT-Verantwortlichen, Ihren Kolleginnen und Kollegen oder Ihren Vorgesetzten über mögliche Schwachstellen in Ihrem Unternehmen und tragen Sie dadurch zu mehr Sicherheit bei!

KommR Robert Bodenstein, MBA CMC
Bundesspartenobmann

1. Sicherer Umgang mit Computern und Informationen

Informationen sind das Kapital jedes Unternehmens. Alle Mitarbeiterinnen und Mitarbeiter müssen über den Wert der Information Bescheid wissen. Der Missbrauch von Daten kann Wettbewerbsnachteile, Umsatzeinbußen, Imageverluste oder rechtliche Probleme zur Folge haben. Daher ist es besonders wichtig, Informationen und Computer vor unberechtigter Verwendung zu schützen.

Heute verfügen die meisten Unternehmen bereits über technische Sicherheitsmechanismen, die den Zugriff auf Daten regeln. Allerdings gibt es in vielen Unternehmen keine klaren Regelungen, wie Daten verwendet werden sollen (z.B. deren Weitergabe, Vervielfältigung, Verarbeitung oder Löschung).

SICHERER UMGANG MIT PERSONENBEZOGENEN DATEN

Der Umgang mit personenbezogenen Daten – diese können natürlichen, aber auch juristischen Personen zugeordnet werden – wird durch das österreichische Datenschutzgesetz (DSG 2000) geregelt. Dieses Gesetz stellt alle personenbezogenen Daten, insbesondere aber auch „sensible personenbezogene Daten" (zu Rasse und ethnischer Herkunft, politischer Meinung, Gewerkschaftszugehörigkeit, religiöser oder philosophischer Überzeugung, Gesundheit oder Sexualleben) unter besonderen Schutz. Weiters legt es fest, dass alle personenbezogenen Daten nur zu festgelegten Zwecken und aufgrund einer ausdrücklichen Anordnung des Dienstgebers verwendet und weitergegeben werden dürfen.

Ab 25. Mai 2018 wird das Datenschutzgesetz 2000 durch die EU-Datenschutz Grundverordnung (kurz: DSGVO) und das Datenschutzanpassungsgesetz 2018 ersetzt. Die Datenschutz-Grundverordnung ist zwar als EU-Verordnung in jedem EU-Mitgliedstaat unmittelbar anwendbar, sie enthält jedoch zahlreiche Öffnungsklauseln und lässt dem nationalen Gesetzgeber gewisse Spielräume. Es gibt daher auch eine Novelle des österreichischen Datenschutzgesetzes 2000 (das „Datenschutz-Anpassungsgesetz 2018"). Bis zum 25. Mai 2018 müssen daher alle Datenanwendungen im Betrieb an die neue Rechtslage angepasst werden.

Bitte beachten Sie folgende Hinweise:

- Sie müssen personenbezogene Daten, die Ihnen aufgrund Ihrer beruflichen Tätigkeit anvertraut wurden, geheim halten.
- Ihr Arbeitgeber muss Ihnen klare Anweisungen geben, auf welche Weise diese Daten verarbeitet bzw. an welche andere Personen oder Unternehmen sie weitergegeben werden dürfen. Jede andere Nutzung oder Weitergabe personenbezogener Daten ist nicht erlaubt.
- Der Arbeitgeber hat Sie über Ihre Pflichten nach dem DSG 2000 (ab Mai 2018 nach dem DSG und der DSGVO) sowie den internen Vorschriften zu belehren.
- Nach dem Ausscheiden aus dem Betrieb oder dem Wechsel der Arbeitsstelle dürfen Sie personenbezogene Daten, die Ihnen beruflich zugänglich gemacht wurden, nicht weitergeben oder für andere Zwecke nutzen.

Verstöße gegen das Datenschutzrecht werden mit hohen Geldstrafen für Ihr Unternehmen geahndet und können auch für Sie arbeitsrechtliche Konsequenzen haben. Zusätzlich können Geschädigte Schadenersatz einklagen. Dazu kommt noch der Vertrauensverlust bei Kunden und Geschäftspartnern.

Es ist daher empfehlenswert, bei der Verwendung personenbezogener Daten besondere Vorsicht walten zu lassen. Sie müssen so gespeichert werden, dass sie für unberechtigte Personen nicht zugänglich sind.

CLEAR DESK POLICY

Clear Desk-Policy bedeutet, dass die Mitarbeiterinnen und Mitarbeiter alle vertraulichen Unterlagen bei Abwesenheit verschließen, sodass unberechtigte Personen (Besucherinnen und Besucher, Reinigungspersonal, aber auch unbefugte Kolleginnen und Kollegen etc.) keinen Zugriff darauf haben. Dies gilt insbesondere für Großraumbüros oder Räume mit Publikumsverkehr.

Bitte beachten Sie folgende Hinweise:

- Achten Sie darauf, dass Computerausdrucke oder Kopien mit sensiblen Informationen nicht für Unbefugte frei zugänglich herumliegen, z.B. neben dem Drucker oder im Kopierer. Solche Dokumente müssen sicher verwahrt oder zuverlässig vernichtet werden.

- Versperren Sie Schriftstücke oder Datenträger mit vertraulichen Inhalten an einem sicheren Ort (Schreibtisch, versperrbare Kästen, Datenträgersafe)!
- Bewahren Sie unter keinen Umständen Passwortnotizen an Ihrem Arbeitsplatz auf (unter der Schreibtischunterlage, als Post-it am Bildschirm)!
- Sperren Sie Ihren Computer, wenn Sie Ihren Arbeitsplatz für längere Zeit verlassen (z. B. unter Windows mit „Windows-Taste + L“)! Unbeaufsichtigte, nicht gesperrte Computer sind ein hohes Sicherheitsrisiko. Unbefugte könnten so Zugang zu vertraulichen Daten erhalten.
- Konfigurieren Sie einen Bildschirmschoner, der sich nach maximal fünf Minuten aktiviert und nur durch Eingabe eines Passworts aufzuheben ist. Falls bereits ein passwortgeschützter Bildschirmschoner installiert ist, deaktivieren Sie ihn nicht!
- Richten Sie Ihr Smartphone oder Tablet so ein, dass es nur nach Eingabe einer PIN oder eines Passworts verwendet werden kann. Lassen Sie es nicht entsperrt liegen und geben Sie es nicht unbeaufsichtigt an Andere weiter!

DATENTRÄGER UND PAPIERDOKUMENTE RICHTIG ENTSORGEN

Computer, Datenträger und Papierdokumente mit vertraulichen oder personenbezogenen Inhalten, die defekt geworden sind oder nicht mehr benötigt werden, müssen auf sichere Art entsorgt werden. Sorglos weggeworfene Dokumente oder liegengelassene Kopien können ein ernstes Sicherheitsproblem darstellen, wenn diese Dokumente in falsche Hände geraten und missbräuchlich verwendet werden.

Bitte beachten Sie folgende Hinweise, wenn Sie Papierdokumente oder Datenträger wie z.B. USB-Sticks, Festplatten, Speicherkarten, CDs/DVDs, Mikrofiches und Sicherungsbänder entsorgen:

- Werfen Sie Datenträger auf keinen Fall in den Papierkorb! Sofern es sich um Inhalte handelt, die Außenstehenden nicht zugänglich gemacht werden dürfen, müssen die Datenträger sicher entsorgt werden. Beachten Sie, dass diese Vorgehensweise auch bei Archivmaterial einzuhalten ist.
- Übergeben Sie die nicht mehr benötigten Datenträger den Verantwortlichen Ihrer EDV-Abteilung bzw. einer eigens zu diesem Zweck bestimmten Person, die für die sichere Entsorgung zuständig ist.
- Wenn Sie eine Festplatte verkaufen oder entsorgen wollen, müssen Sie vorher alle Inhalte mit einer geeigneten Löschsoftware löschen. Das Formatieren der Festplatte ist nicht ausreichend! Verwenden Sie stattdessen ein Programm wie Eraser oder Disk Wipe. Beide Programme sind kostenlos und bieten sichere Methoden zur endgültigen Bereinigung Ihrer Datenträger.
- Für USB-Sticks, Solid State-Disks und Speicherkarten sind die oben genannten Programme nicht geeignet! Neuere Modelle können über den Befehl „Secure Erase“ zuverlässig gelöscht werden, bei vielen älteren Typen ist aber kein sicheres Löschen möglich. Solche Datenträger dürfen nicht verkauft oder entsorgt werden, wenn sie für das Speichern Ihrer sensiblen Daten verwendet wurden. Sie sollten daher von Anfang an alle Daten auf diesen Speichermedien verschlüsseln: Ohne Ihren Benutzerschlüssel sind sie – auch ohne Löschen – unlesbar.
- Optische Datenträger (CDs, DVDs) können nur „gelöscht“ werden, indem man sie physisch zerstört. Man kann sie also in möglichst kleine Teile zerbrechen oder die Beschichtung auf der Beschriftungsseite großflächig abkratzen. Meistens ist es aber einfacher, solche Medien zu sammeln und zum Shreddern an ein geeignetes Entsorgungsunternehmen zu übergeben. Beispiele für die korrekte Entsorgung finden Sie auf http://www.zendas.de/themen/vernichtung/beispiele_cddvd.html.
- Entsorgen Sie Papierdokumente mit sensiblen Informationen nicht mit dem Altpapier! Kleinere Mengen können Sie mit einem handelsüblichen Aktenvernichter (Shredder), größere Mengen über ein Entsorgungsunternehmen vernichten.
- Achten Sie darauf, dass bei Verlassen von Besprechungsräumen sämtliche sensiblen Informationen (z.B. auf Flipcharts) entfernt oder mitgenommen werden.
- Stellen Sie sicher, dass Sie nach dem Kopieren sämtliche Dokumente vom Kopiergerät entfernt haben und entsorgen Sie unbenötigte Dokumente mit vertraulichem Inhalt auf sichere Art.

SICHERER UMGANG MIT MOBILEN IT-GERÄTEN

Der Einsatz mobiler IT-Geräte (Notebooks, Smartphones, Tablet-PCs) birgt erhebliche Gefahren für das Unternehmen: Vertrauliche Unternehmensdaten werden außerhalb des Unternehmens gespeichert und verwendet. Portable Geräte sind für Diebe eine attraktive, leicht zu verkaufende Beute.

Wenn Sie mobile IT-Geräte benutzen, sollten Sie Folgendes beachten:

- Sorgen Sie für eine diebstahlsichere Aufbewahrung Ihres Gerätes. Bewahren Sie es grundsätzlich nicht im Fahrzeug auf. Ist dies nicht zu vermeiden, decken Sie das Gerät ab oder schließen Sie es im Kofferraum ein.
- Lassen Sie das Gerät nicht unbeaufsichtigt und überlassen Sie es nicht anderen Personen! Sperren Sie es bei kurzen Arbeitspausen oder schalten Sie es ab. Stellen Sie es so ein, dass es nur nach Überwinden einer Zugriffschutzfunktion (Passwort, PIN, Fingerprint, ...) bedient werden kann.
- Es gibt verschiedene Programme und Dienste, die es erlauben, alle Daten auf einem gestohlenen oder verlorenen Smartphone aus der Distanz zu löschen. Setzen Sie diese Apps unbedingt ein! Auch der Einsatz von Virenschutzprogrammen für Smartphones und Tablets ist dringend anzuraten.
- Falls Sie Ihr eigenes Smartphone oder Tablet für berufliche Zwecke einsetzen wollen: Klären Sie zuvor mit Ihren IT-Zuständigen und Vorgesetzten ab, ob diese Verwendung in Ihrem Unternehmen zugelassen ist. Stellen Sie gemeinsam sicher, dass alle notwendigen Sicherheitsmaßnahmen umgesetzt wurden!
- Falls Ihr Unternehmen eine Mobile Device Management-Lösung einsetzt: Verwenden Sie für berufliche Zwecke ausschließlich die dafür vorgesehenen Anwendungen und verarbeiten Sie keine dienstlichen Daten im privaten, ungeschützten Bereich!
- Vermeiden Sie kostenlose, öffentlich zugängliche WLAN-Netzwerke, wenn Sie Mobilgeräte für berufliche Zwecke einsetzen: Ihre unverschlüsselte Kommunikation über das Netzwerk kann problemlos abgehört werden. Im schlimmsten Fall können auch Daten auf Ihrem Gerät ausgelesen werden.
- Sorgen Sie für Sichtschutz, wenn Sie das Gerät in der Öffentlichkeit verwenden (z.B. am Flughafen) – das verhindert das Ausspähen von Unternehmensinformationen.
- Verschlüsseln Sie die Festplatteninhalte bzw. wichtige Dateien und verhindern Sie damit unbefugten Zugriff auf Firmendaten. Aktivieren Sie auch auf Ihrem Smartphone oder Tablet die Dateiverschlüsselung oder setzen Sie eine Verschlüsselungs-App zum Speichern sensibler Daten ein!

- Verwenden Sie Ihren privaten Cloud-Speicherdienst (Dropbox, iCloud, Google Drive) nicht für Unternehmensdaten! Fragen Sie bei Ihren IT-Zuständigen nach, welche Möglichkeiten bestehen, um Firmendokumente über das Internet sicher abzuspeichern.
- Deaktivieren Sie alle nicht gerade benötigten Geräteschnittstellen (USB, WLAN, Infrarot, Bluetooth). Wenn diese Schnittstellen (z.B. WLAN für Internetverbindung) unbedingt notwendig sind, müssen entsprechende Schutzmaßnahmen (Personal Firewall, aktuelles Virenschutzprogramm usw.) vorgesehen werden.
- Schalten Sie den GPS-Empfänger auf Ihrem Smartphone immer ab, wenn er nicht gebraucht wird.
- Auf Smartphones oder Tablets, die Sie für berufliche Zwecke verwenden, dürfen Sie nie interne Sicherheitsmechanismen außer Kraft setzen (z.B. „Jailbreaks“ oder “Rooten“)! Durch diese Manipulationen entstehen zusätzliche Gefahrenquellen für die gespeicherten Unternehmensdaten.
- Installieren Sie nur Apps, die Ihnen als vertrauenswürdig und sicher bekannt sind! Fragen Sie im Zweifelsfall Ihre IT-Zuständigen oder recherchieren Sie im Internet, ob dazu Gefahren bekannt sind.
- Viele Apps verlangen bei der Installation Zugriff auf verschiedenste Gerätefunktionen (WLAN, GPS-Empfänger…). Überlegen Sie selbst, ob es nötig ist, dass z.B. eine Spiele-App Zugriff auf Ihr Mikrophon oder Ihr Adressbuch erhält. Installieren Sie nur Apps, deren Zugriffsanforderungen Sie für vertrauenswürdig halten!
- Lassen Sie Ihr Smartphone bei vertraulichen Besprechungen an Ihrem Arbeitsplatz oder schalten Sie es in den Flugmodus!
- Bevor Sie ein Smartphone verkaufen, weitergeben oder entsorgen, müssen Sie sicherstellen, dass alle gespeicherten Daten gelöscht wurden. Am besten eignet sich dazu ein „Factory Reset“. Danach müssen Sie überprüfen, ob noch Einstellungen oder Daten erhalten geblieben sind.
- Melden Sie jeden Diebstahl oder Verlust sofort der IT-Abteilung! Möglicherweise müssen Fernzugänge zu Ihrem Unternehmen gesperrt oder Passwörter geändert werden, um unerlaubte Zugriffe zu unterbinden. Die rasche Meldung des Vorfalls kann helfen, weitere Sicherheitsverstöße zu verhindern.
- Wenn auf dem Mobilgerät personenbezogene Daten gespeichert waren, muss unverzüglich abgeklärt werden, ob Ihr Arbeitgeber die Datenschutzbehörde und die betroffenen Personen informieren muss. Ihre rechtzeitige Meldung kann dem Unternehmen daher unter Umständen hohe Geldstrafen ersparen.

WECHSELMEDIEN RICHTIG VERWENDEN

Wechselmedien sind externe Datenträger wie z.B. USB-Sticks, externe Festplatten, Fotospeicherkarten, CDs oder DVDs. Ihr Einsatz stellt grundsätzlich ein Sicherheitsrisiko dar: Einerseits können bei Missbrauch sensible Daten wie z.B. Kundenkarteien gelesen werden, andererseits können Programme mit Schadfunktionen auf Firmenrechner bzw. in das Firmennetzwerk eingeschleust werden.

Wenn Wechselmedien in Ihrem Unternehmen verwendet werden, sollten Sie folgende Hinweise (zusätzlich zu allfälligen Regelungen Ihres Unternehmens) beachten:

- Lassen Sie Wechseldatenträger wie z.B. USB-Sticks nie unbeaufsichtigt liegen!
- Setzen Sie unbedingt Verschlüsselungs- oder Sperrfunktionen ein! Häufig liegt dem USB-Stick eine Verschlüsselungssoftware bei, die gespeicherte Daten mittels Passwort schützt. Auch alle modernen Betriebssysteme bieten Möglichkeiten zur Datenträgerverschlüsselung an.
- Einige Verschlüsselungsprogramme bieten die Möglichkeit, den Inhalt des USB-Sticks nach mehrmaliger falscher Passworteingabe automatisch zu löschen. Besonders bei sensiblen Inhalten sollten Sie diese Möglichkeit nützen.
- Booten Sie Ihren Rechner nicht von einem Wechseldatenträger! Auch das Starten nicht freigegebener Programme von USB-Sticks (z.B. portable Versionen von Browsern oder E-Mail-Clients) ist nicht erlaubt. Sie können damit Viren oder andere Schadsoftware in Ihren Computer einschleppen, die sich auf das gesamte Unternehmen ausbreiten.
- Auch für Wechseldatenträger gilt: Jeder Verlust muss sofort gemeldet werden!

TIPP:

Die Installation privater Software kann einzelne PCs oder das gesamte Firmennetz bedrohen! Besonders kostenlose Software aus dem Internet (z.B. Spiele, „nützliche“ Tools und Apps) enthält oft Schadprogramme. Zudem könnte das Urheberrecht verletzt werden, wenn diese Programme nicht für den kommerziellen Einsatz lizenziert oder illegal kopiert wurden.

SOCIAL ENGINEERING

Social Engineering bezeichnet das Manipulieren von Personen, um unbefugt Zugang zu vertraulichen Informationen oder IT-Systemen zu erhalten. Typisches Werkzeug des Social Engineers ist das Telefon. Persönliches Auftreten wird wegen des höheren Risikos zumeist gescheut, kommt aber ebenfalls vor.

STRATEGIE DES SOCIAL ENGINEERS

Social Engineers geben sich gerne als Mitarbeiterinnen oder Mitarbeiter aus. Vielleicht behaupten sie auch, eine Behörde oder ein wichtiges Kundenunternehmen zu vertreten oder zu Ihrer IT-Abteilung zu gehören. Ihre Opfer werden durch firmeninternes Wissen oder Kenntnisse spezieller Fachbegriffe getäuscht, die sie sich zuvor durch Telefonate oder Gespräche mit anderen Kollegen erworben haben. Beim Angriff appellieren sie dann als „gestresster Kollege" an Ihre Hilfsbereitschaft oder drohen als „Kunde" mit dem Verlust eines Auftrages. Kommt ein Social Engineer bei einer Mitarbeiterin oder einem Mitarbeiter nicht ans Ziel, wird der Angriff bei der nächsten Ansprechperson wiederholt – bis er erfolgreich ist.

Häufig verlaufen diese Angriffe mehrstufig:

- Durch gezielte Telefonate werden Insiderinformationen eingeholt, die an sich harmlos sind, deren Kenntnis dem Social Engineer aber hilft, seine Rolle überzeugend zu spielen.
- Oft wird über längere Zeit ein Vertrauensverhältnis aufgebaut, indem die Angreiferin oder der Angreifer z.B. mehrere Telefonate mit ihrem oder seinem Opfer führt und unproblematische Anfragen stellt.
- Der eigentliche Angriff erfolgt nach diesen Recherchen: Wenn die Opfer den „Kollegen" oder „Kunden" gut zu kennen glauben, geht der Social Engineer zu seinem eigentlichen Ziel über – und bittet um den entscheidenden „Gefallen".

Oft wird ein solcher Angriff nicht einmal bemerkt. Der Social Engineer bleibt unerkannt und kann die anfälligen Mitarbeiterinnen und Mitarbeiter bei anderer Gelegenheit wieder nach vertraulichen Informationen aushorchen.

WER BESONDERS GEFÄHRDET IST

Social Engineering-Attacken können sich gegen jede Person im Unternehmen richten. Am stärksten gefährdet sind

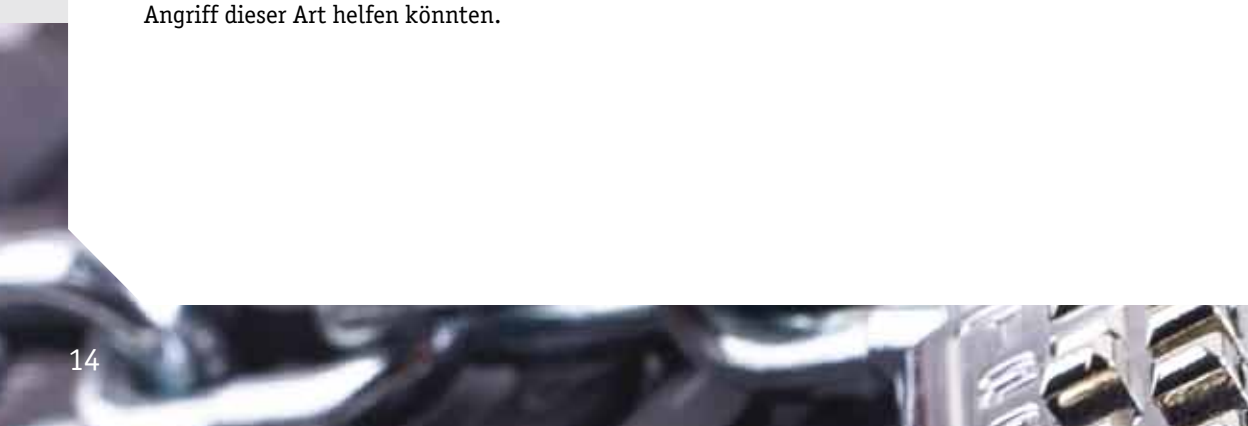
- neue Mitarbeiterinnen und Mitarbeiter, die mit den Verhältnissen noch nicht vertraut sind;
- Personen im Kundenverkehr, da sie besonders kundenorientiert arbeiten. Hier finden sich außerdem häufig mehrere Ansprechpersonen mit gleichen Zugriffsrechten, sodass der Social Engineer einen fehlgeschlagenen Angriff bei einem anderen Opfer wiederholen kann.

MASSNAHMEN GEGEN SOCIAL ENGINEERING

Angriffe dieser Art können nie völlig unterbunden werden. Bitte beachten Sie aber folgende Vorsichtsmaßnahmen:

- Informieren Sie sich über den Wert und Vertraulichkeitsgrad der Informationen, zu denen Sie Zugang haben!
- Häufig ist Unternehmensangehörigen infolge des dauernden Umgangs mit sensiblen Informationen nicht mehr bewusst, dass diese geheim sind. Auch fehlen oft klare Regelungen der Geschäftsführung. In jedem Unternehmen sollte – am besten in schriftlicher Form – festgelegt sein, welche Informationen vertraulich zu behandeln sind und welche weitergegeben werden dürfen. Sollte dies in Ihrem Unternehmen nicht der Fall sein, regen Sie eine solche Festlegung an oder klären Sie diesen Bereich zumindest mit Ihren Vorgesetzten.
- Bestehen Sie bei Anfragen zu vertraulichen oder geheimen Informationen auf schriftliche Form oder persönliche Vorsprache!
- Geben Sie über anonyme Kanäle (Telefon, E-Mail, Postfächer) grundsätzlich keine vertraulichen Informationen weiter!

Vertrauliche Informationen in diesem Sinn sind nicht nur Passwörter, Kontodaten oder ähnliche sensiblen Daten, sondern auch Firmeninterna wie z.B. Abläufe oder Fachwörter, die bei einem Angriff dieser Art helfen könnten.



- Legen Sie im Vorhinein Methoden fest, wie die Identität von Anfragestellern sicher festgestellt werden kann: Reicht z.B. die Kundennummer oder ist ein zusätzliches Passwort nötig? So lässt sich Zeitdruck vermeiden, der gern als Hilfsmittel bei Social Engineering-Angriffen eingesetzt wird.
- Gibt eine Person vor, Mitarbeiterin oder Mitarbeiter eines bestimmten Unternehmens zu sein, sollten Sie bei diesem Unternehmen anfragen, ob die betreffende Person überhaupt existiert. Dazu muss aber die Telefonnummer aus öffentlichen Quellen (z.B. amtliches Telefonbuch) abgefragt werden – verwenden Sie nicht jene Telefonnummer, die die Person angegeben hat.
- Wenn Sie sich bei einer Anfrage nicht sicher sind oder wenn die oder der Anfragende versucht, Sie unter Druck zu setzen, leiten Sie die Anfrage an Ihre Vorgesetzten weiter! Einschüchterungsversuche dieser Art gehören zum Standardrepertoire des Social Engineering.
- Wenn Sie im Anschluss an ein Gespräch „ein unangenehmes Gefühl" haben oder unsicher sein, ob Sie nicht „zu viel gesagt" haben, behalten Sie Ihre Sorgen nicht für sich, sondern sprechen Sie mit Ihren Vorgesetzten darüber! Möglicherweise müssen Abwehrmaßnahmen getroffen oder die betroffenen Personen informiert werden. In jedem Fall müssen Sie informiert werden, wie Sie bei derartigen Fällen vorgehen sollen.

TIPP:

Besprechen Sie mit Ihren Kolleginnen und Kollegen auffällige oder unzulässige Anfragen und dokumentieren Sie diese Anfragen. So weiß man, ob die Anruferin oder der Anrufer es schon bei anderen versucht hat. In solchen Gesprächen können auch neue Abwehrmethoden gefunden und ein Gefühl für den Wert der Firmeninformationen entwickelt werden.

2. Passwörter – richtig auswählen und verwalten

Passwörter dienen dem Schutz von IT-Geräten und Daten und verhindern unbefugte Zugriffe. Deswegen sind die richtige Auswahl und der richtige Umgang wichtig: Passwörter müssen komplex sein und geheimgehalten werden.

DIE RICHTIGE AUSWAHL

Beachten Sie bei der Auswahl Ihres Passwortes:

- Ein gutes Passwort besteht aus mindestens zehn verschiedenartigen Zeichen. Es muss Großbuchstaben, Kleinbuchstaben, Ziffern und/oder Sonderzeichen (Satzzeichen, Währungssymbole etc.) enthalten. Nur Klein- und Großbuchstaben zu verwenden ist unsicher!
- Niemals Namen, Vornamen, Geburtsdaten, Tel.-Durchwahlen, KFZ-Kennzeichen etc. verwenden. Diese werden bei Angriffen zuerst ausprobiert.
- Verwenden Sie keine Begriffe aus einem Wörterbuch (auch nicht in einer anderen Sprache). Es gibt Programme, die Wortlisten mit mehreren tausend Begriffen sofort abrufen und so mögliche Passwörter finden. Auch Eigennamen, geografische Begriffe etc. dürfen nicht verwendet werden.
- Trivial-Passwörter (qwertz, aaaaa, 08/15, 4711 etc.) sind ebenfalls ungeeignet. Sie können von Anderen leicht beim Beobachten der Passworteingabe erkannt werden.

TIPP:

Bilden Sie Ihr Passwort aus den Wortanfängen und Satzzeichen einfacher Merksätze. Ein Satz wie „Ich kann mir nur ein Passwort leicht merken!“ wird zum Passwort: „Ikmn1PWlm!“.

DER RICHTIGE UMGANG

Geben Sie Ihre Passwörter – insbesondere das Passwort für das Anmelden am Computer – nicht an Ihre Kolleginnen und Kollegen oder an Ihre Vorgesetzten weiter. Sollte die Weitergabe unbedingt notwendig sein, ändern Sie Ihr Passwort anschließend sofort.

Setzen Sie für verschiedene Anmeldungen verschiedene Passwörter ein! Durch kleine Variationen – indem Sie z.B. drei Buchstaben Ihres Passworts ändern – ist dies leicht durchführbar und bleibt einfach zu merken.

Auf keinen Fall dürfen Sie das gleiche Passwort für die Anmeldung am Firmen-PC und Anmeldungen im Internet (z.B. dem E-Mail-Konto bei einem Internet-Provider) verwenden. Wenn es in falsche Hände gerät, kann es gegen Ihr Unternehmen eingesetzt werden: Es gibt Fälle, wo Benutzer auf Webseiten gelockt und zur Angabe einer E-Mail-Adresse und eines Passworts aufgefordert wurden – in der (kriminellen) Hoffnung, dass das Opfer aus Bequemlichkeit keine unterschiedlichen Passwörter verwendet.

PASSWORT-MANAGER VERWENDEN

Mit einem Passwort-Manager können mehrere, unterschiedliche Passwörter verwaltet und durch ein einziges Master-Passwort geschützt werden. Dieses Passwort muss sicher sein, also zumindest die obigen Kriterien erfüllen. Manche Passwort-Manager generieren auch auf Knopfdruck sichere Passwörter.

Wenn Sie in Ihrem Internet-Browser einen integrierten Passwort-Manager verwenden, aktivieren Sie bitte die Option „Master Passwort“. Dann können Sie ein sicheres Master-Passwort wählen.

Sie finden im Internet eine Reihe kostenloser Passwort-Manager. Verschiedene Websites, auf denen Sie den Sicherheitsgrad Ihrer Passwörter testen und überprüfen können, sind mit einer Internet-Suche nach „Passworttest“ leicht zu finden.

3. Sicher unterwegs im Internet

Ebenso wie im realen Leben ist man auch im Internet mit Kriminellen und Betrügern konfrontiert. Es liegt in Ihrer eigenen Verantwortung, solche Bedrohungen zu erkennen und entsprechend darauf zu reagieren.

VORSICHTSMASSNAHMEN

Einige einfache Verhaltensregeln reichen aus, um typische Gefahren zu minimieren:

- Gebrauchen Sie Ihren gesunden Menschenverstand: Websites, die von bekannten und angesehenen Anbietern ins Netz gestellt werden, ist eher zu vertrauen als unbekannten Seiten.
- Websites, die mit dem Download kostenloser Zusatzsoftware oder unseriösen Gewinnspielen locken, ist grundsätzlich zu misstrauen. Natürlich gibt es auch seriöse Anbieter von kostenlosen Free- und Shareware-Programmen im Internet. Sollten Sie sich aber nicht sicher sein, fragen Sie bei Ihren Vorgesetzten oder EDV-Verantwortlichen nach.
- Vor dem Download von Zusatzprogrammen – auch bei scheinbar ungefährlichen Dingen wie Bildschirmschonern, Klingeltönen oder Mauszeigern – ist grundsätzlich die Zustimmung Ihrer Vorgesetzten oder EDV-Verantwortlichen einzuholen.
- Das Herunterladen von Dateien kann – abgesehen von der Gefahr des Einschleppens von Schadsoftware – auch zu lizenz- und urheberrechtlichen Problemen führen. Das gilt auch für Software, die nicht installiert oder ausgeführt wurde und nur auf dem Bürorechner gespeichert ist. Holen Sie daher vorher die Zustimmung Ihrer Vorgesetzten oder EDV-Verantwortlichen ein.
- Meiden Sie Hackerseiten und solche, auf denen kommerzielle Software, möglicherweise in gecrackter Form, zum Download angeboten wird (sogenannte „Warez"-Seiten). Die Wahrscheinlichkeit, dadurch Schadsoftware auf den Computer zu laden, ist naturgemäß deutlich höher als beim Aufsuchen der Website einer Bank oder eines bekannten Unternehmens. „Verdächtige" Seiten sollten Sie am besten gar nicht aufrufen.
- Rufen Sie keine Websites mit pornografischen, gewaltverherrlichenden oder strafrechtlich bedenklichen Inhalten auf. Das kann gravierende rechtliche Probleme – auch für Ihr Unternehmen – nach sich ziehen.

Bei der Nutzung von Sozialen Netzwerken sind besondere Vorsichtsmaßnahmen zu berücksichtigen:

Soziale Netzwerke, wie Facebook, Xing oder Twitter, erfreuen sich großer Beliebtheit. Viele Plattformen bieten Netzwerke für spezifische Themenbereiche an. Leider nützen aber auch Kriminelle diese Plattformen für ihre Zwecke. Daher sind mit der Benutzung sozialer Netzwerke auch Risiken verbunden. Neben dem Diebstahl persönlicher Daten und dem Verbreiten von Spam oder Schadsoftware sammeln immer mehr Angreifer Informationen, die Nutzerinnen und Nutzer der Plattformen über sich und ihr Umfeld preisgeben. Diese Informationen erlauben es, gezielte Angriffe auf Unternehmen durchzuführen, indem etwa personalisierte Phishing-Mails an Geschäftsführung, Vertrieb oder Buchhaltung verschickt werden oder maßgeschneiderte Schadsoftware Firmengeheimnisse ausspioniert oder zerstört.
Bedenken Sie die möglichen arbeitsrechtlichen Konsequenzen: Wenn Sie vertrauliche Informationen des Unternehmens preisgeben oder das Unternehmen durch Ihre Aussagen in Verruf bringen, kann dies als Verletzung Ihrer Treuepflicht gedeutet. Wenn Sie das Sicherheitsrisiko bei der Nutzung sozialer Netzwerke minimieren wollen, sollten Sie einige grundlegende Sicherheitshinweise beachten:

- Informieren Sie sich, ob in Ihrem Unternehmen die Nutzung sozialer Netzwerke während der Arbeitszeit gestattet ist.
- Das Netz vergisst nie! Denken Sie immer daran, dass Informationen, die Sie auf sozialen Netzwerken preisgeben, öffentlich sind und oft nur schwer wieder gelöscht werden können.
- Vermeiden Sie es, vertrauliche Informationen über Ihr Unternehmen, Ihre berufliche Rolle oder Ihre geschäftliche Tätigkeit zu veröffentlichen. Alle diese Daten können bei Angriffen genutzt werden, um Sicherheitsvorkehrungen zu umgehen.
- Unterscheiden Sie zwischen Ihrem geschäftlichen und Ihrem privaten Ich und verwenden Sie unterschiedliche Plattformen oder Profile. Private Daten haben auf Geschäftsprofilen nichts verloren und umgekehrt. Damit erschweren Sie den Missbrauch Ihrer Daten für Angriffe und schützen zudem noch Ihre Privatsphäre.
- Prüfen Sie unbedingt die Identität der anfragenden Person, bevor Sie diese zu Ihrem Netzwerk hinzufügen.
- Nutzen Sie die Sicherheits- und Datenschutzoptionen, die vom Plattformanbieter zur Verfügung gestellt werden und schränken Sie den Zugang zu Ihrem Profil ein. Kontrollieren Sie regelmäßig, ob der Betreiber Veränderungen vorgenommen hat, die unerwünschte Zugriffe ermöglichen.
- Vorsicht bei externen Links: Bedenken Sie, dass soziale Netzwerke oft genutzt werden, um Schadsoftware zu verbreiten.
- Verwenden Sie auch in sozialen Netzwerken ein sicheres Passwort!

VERSCHLÜSSELTE DATENÜBERTRAGUNG

Die Datenübertragung zwischen Servern im Internet und Ihrem PC erfolgt im Normalfall unverschlüsselt. Daher können übertragene Daten von Personen mit entsprechenden Zugangsmöglichkeiten problemlos abgehört oder manipuliert werden. Um dies bei der Übertragung sensibler Daten zu verhindern, wurde das Protokoll HTTPS mit dem Verschlüsselungsprotokoll TLS/SSL entwickelt. Dadurch sind folgende Sicherheitsmerkmale gewährleistet:

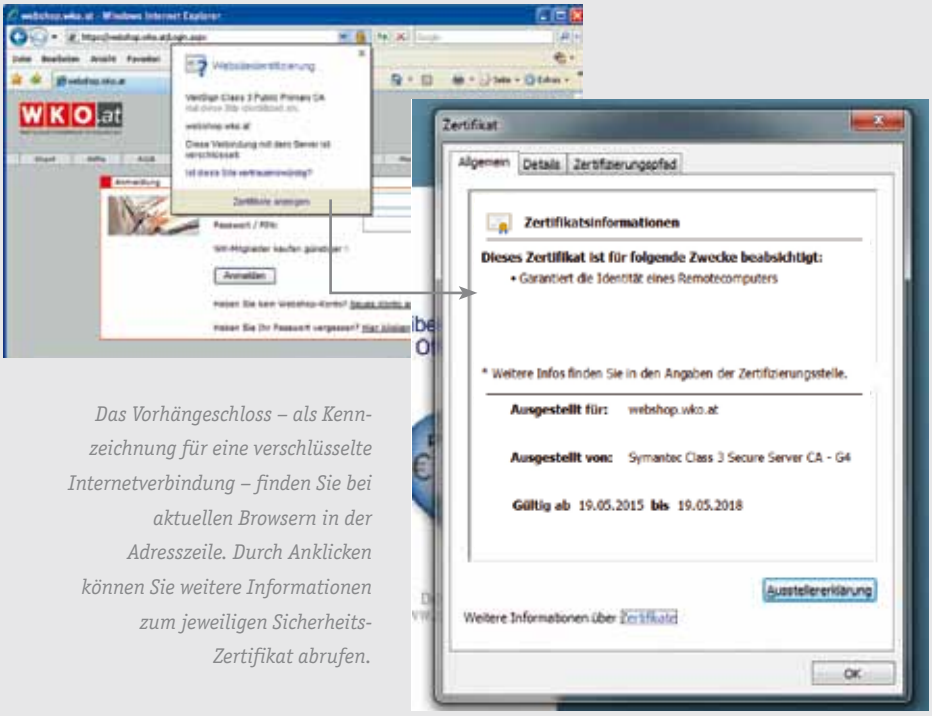
- Die übertragenen Daten werden verschlüsselt und sind für Außenstehende nicht lesbar.
- Die Identität des Webservers, der die Daten verarbeitet, wird anhand eines digitalen Zertifikats geprüft.
- Die übertragenen Daten werden durch verschiedene Rechenverfahren geprüft und vor Manipulationen geschützt.

SICHERHEIT DURCH DIGITALE ZERTIFIKATE

Das wichtigste Element einer HTTPS-Verbindung ist das digitale Zertifikat des Website-Betreibers. Dieses Zertifikat wird vom Internet-Browser verwendet, um die Identität des Website-Betreibers festzustellen. Dadurch kann verhindert werden, dass eine gesicherte Verbindung zu einem Anbieter aufgebaut wird, der sich als jemand anderer ausgibt (z.B. einem Betrüger, der die Website einer Bank nachbaut, um Kunden ihre Passwörter zu entlocken).

Folgende Vorsichtsmaßnahmen sollten bei HTTPS-Verbindungen beachtet werden:

- Besondere Vorsicht ist geboten, wenn der Internet-Browser auf Schwierigkeiten mit dem Zertifikat hinweist. Er zeigt damit an, dass er den Aussteller des Zertifikats nicht kennt, dass das Zertifikat abgelaufen oder unsicher ist, oder dass der Name im Zertifikat nicht zur Website passt. Oft sind diese Meldungen nicht leicht zu interpretieren. Deswegen sollten Sie entweder Ihre IT-Verantwortlichen oder besser noch kompetente Mitarbeiterinnen oder Mitarbeiter des Unternehmens, dessen Website Sie besuchen wollen, um Rat fragen.



Das Vorhängeschloss – als Kennzeichnung für eine verschlüsselte Internetverbindung – finden Sie bei aktuellen Browsern in der Adresszeile. Durch Anklicken können Sie weitere Informationen zum jeweiligen Sicherheits-Zertifikat abrufen.

TIPP:

Kontrollieren Sie die Internet-Adresse genau, um kriminellen Methoden vorzubeugen. Es gab bereits Betrugsfälle, in denen die Opfer auf ähnlich aussehende URLs gelockt wurden (http://ebanking.bawog.com anstelle von https://ebanking.bawag.com, http://www.paipal.com statt https://www.paypal.com). Durch die Kontrolle der Adresszeile im Browser können Sie diesen Betrug erkennen.

TRACKING COOKIES

Cookies sind sehr kleine Dateien, die beim Besuch einer Website auf Ihrem Computer gespeichert werden. Wenn Sie diese Website wieder aufrufen, darf sie ihre eigenen Cookies lesen. Auf diese Weise lassen sich bestimmte Einstellungen speichern, zum Beispiel Ihre Identität nach einer Web-Anmeldung oder Ihr Warenkorb in einem Online-Shop.

Sehr viele Websites setzen aber auch sogenannte „Tracking Cookies" ein, die von großen Werbeanbietern wie Google oder Facebook erstellt und ausgewertet werden. Damit lassen sich Internetzugriffe über mehrere Websites hinweg verfolgen. Die Werbeanbieter können damit Bewegungsprofile einzelner User im Internet erstellen und für gezielte Werbung verwenden. Wenn Sie ein Google Plus- oder Facebook-Konto besitzen, können sie sogar Ihre Identität bestimmen und diesen „Bewegungsprofilen" zuordnen.

Das ist völlig legal – sofern Sie diesen Cookies zustimmen. Viele Websites bieten Ihnen aber gar nicht die Möglichkeit, sich zu entscheiden. In solchen Fällen bleibt Ihnen nur, bestimmte Einstellungen in Ihrem Browser zu setzen, die das „Tracking" unterbinden:

- Die meisten Browser bieten die Möglichkeit, die besuchten Websites dazu aufzufordern, Ihre Aktivitäten nicht zu verfolgen. Diese Einstellung wird auch als „Do Not Track" bezeichnet. Viele Websites halten sich allerdings nicht an diese Auflage.
- Eine weitere Möglichkeit besteht darin, Cookies regelmäßig zu löschen, z.B. nach jeder Internetsitzung. Das kann recht aufwändig werden; in manchen Browsern lässt es sich aber automatisieren.
- Einige Browser erlauben es, gezielt Cookies von Drittanbietern (das sind fast immer Tracking Cookies) zu blockieren. Die Cookies der besuchten Website sowie Session Cookies bleiben erlaubt, sodass die Funktion der Website dadurch nicht beeinträchtigt wird.
- Guten Schutz gegen Tracking bieten spezielle kostenlose Zusatzprogramme (Add-ons) wie z.B. Ghostery oder uBlock. Diese analysieren den Internetverkehr und blockieren anhand spezieller Listen alle unerwünschten Cookies.

Es ist natürlich einfacher, Tracking einfach zuzulassen. Die Entscheidung darüber sollte aber Ihnen vorbehalten bleiben. Die oben angeführten Einstellungen bieten zusammengenommen eine gute Möglichkeit, die Nachverfolgung Ihrer Internet-Aktivitäten zu unterbinden.

4. E-Mails und Spam

Sicherer Umgang mit unerwünschten Mails

Daten und Informationen werden immer häufiger per E-Mail ausgetauscht. Dadurch landen aber auch Spam-, Hoax- oder Phishing-Mails sowie mit Schadprogrammen verseuchte Nachrichten im Posteingangs-Ordner. Solche unerwünschte Nachrichten – mit mehr oder weniger gefährlichem Inhalt – machen ca. zwei Drittel des weltweiten E-Mail-Aufkommens aus.

UMGANG MIT UNERWÜNSCHTEN E-MAILS

Vor dem Öffnen eingehender E-Mails sollten Sie Folgendes beachten:

- E-Mails im HTML-Format können Skripte mit Schadensfunktion enthalten. Achten Sie auf die Vertrauenswürdigkeit des Absenders und öffnen Sie keine E-Mails, wenn Ihnen Absender oder Betreffzeile verdächtig erscheinen.
- Die meisten Schadprogramme werden aber über Dateien, die als Anhang angefügt sind, übertragen. Office-Dokumente (.docx, .xlsx, .pptx etc.), PDF-Dateien (.pdf), Bildschirmschoner (.scr) und viele andere Dateitypen können Viren enthalten.
- Öffnen Sie daher niemals Dateianhänge, die Ihnen verdächtig vorkommen. Auch bei vermeintlich bekannten und vertrauenswürdigen Absendern ist zu prüfen: Passt der Text der E-Mail zum Absender (englischer Text von deutschsprachigem Absender, unsinniger Text, fehlender Bezug zu aktuellen Vorgängen etc.)? Erwarten Sie die beigelegten Dateien und passen sie zum Absender, oder kommen sie völlig unerwartet?
- Oft ist die Art des Dateianhangs getarnt und über das Icon (z.B. das Word-Symbol) nicht sicher erkennbar. Sie können die Dateianhänge aber problemlos z.B. auf Ihren Desktop kopieren, um sie zu prüfen.
- Kein „Doppelklick“ auf ausführbare Programme (.com, .exe) oder Scripts (.vbs, .bat etc.)! Besonders verdächtig sind doppelte, „merkwürdige“ Dateinamen-Erweiterungen wie beispielsweise .jpg.vbs oder .gif.exe: Sie sollen den Empfängern eine harmlose Bilddatei vortäuschen. Tatsächlich handelt es sich jedoch sehr oft um ein ausführbares Schadprogramm.
- Unerwünschte E-Mails können oft schon daran erkannt werden, dass sie auffällige Rechtschreib- oder Grammatikfehler aufweisen. Häufig stammen sie aus anderen Sprachregionen und wurden nur durch maschinelle Programme übersetzt. Derartige Fehler müssen als Warnsignal gewertet und die betreffende E-Mail mit besonderer Vorsicht behandelt werden.
- Ein weiteres Erkennungsmerkmal betrügerischer E-Mails sind bestimmte „Reizworte“ (Offene Rechnung, Letzte Mahnung, Konto gesperrt, etc.). Offenbar sollen die Empfängerinnen und Empfänger damit unter Druck gesetzt und zu unbedachten Handlungen verleitet werden. Bewahren Sie also die Ruhe und prüfen Sie die E-Mail besonders sorgfältig, bevor Sie einen Dateianhang öffnen oder einen Link anklicken!
- Öffnen Sie keine E-Mails mit Spaßprogrammen, da diese oft Schadfunktionen enthalten.
- Sogenannte Phishing-Mails, die zur Übermittlung von persönlichen Online-Banking-Daten oder Passwörtern (z.B. PIN oder TAN) auffordern, müssen gelöscht werden. Die angeforderten, vertraulichen Informationen dürfen Sie auf keinen Fall weitergeben.

- Oftmals kann in einem E-Mail ein Link angeklickt werden, um eine Webseite aufzurufen. Seien Sie dabei vorsichtig: In betrügerischen E-Mails wird diesen Links oft eine völlig andere Internet-Adresse hinterlegt, als im Mail zu sehen ist. Beim Anklicken wird dann eine gefälschte Phishing-Webseite aufgerufen oder sogar Schadsoftware installiert. Sicherer ist es, den Link mittels „Hyperlink kopieren" in den Browser zu übertragen und ihn vor dem Aufrufen noch einmal zu überprüfen.
- Beantworten Sie keine Spam-Mails! Die Rückmeldung bestätigt dem Spam-Versender nur die Gültigkeit Ihrer Mail-Adresse und erhöht dadurch Ihr Risiko, weitere Zusendungen zu erhalten. Das Abbestellen von E-Mails ist nur bei seriösen Zustellern sinnvoll.
- Benachrichtigen Sie auch Ihre Kolleginnen und Kollegen über verdächtige Zusendungen. Besprechen Sie die aktuellen E-Mails, die Sie als Phishing-Versuche oder Virus-Mails erkannt haben, um gemeinsam die typischen Kennzeichen kennenzulernen. Sie können auf diese Weise sehr rasch Ihre Erkennungsfähigkeit trainieren und verbessern.

Auch bei ausgehenden E-Mails sollte Folgendes beachtet werden (um nicht unabsichtlich Viren zu verteilen oder in Verdacht zu geraten, Spam-Mails zu versenden):

- Prüfen Sie, ob E-Mails im Ausgangs-Postfach stehen, die nicht von Ihnen verfasst wurden. Dies könnte auf Viren hindeuten.
- Versenden Sie keine E-Mails mit z.B. Spaßprogrammen, die Computer-Viren enthalten könnten.
- Folgen Sie nicht den Aufforderungen zur Weiterleitung von Warnungen, Mails oder Dateianhängen an Freunde, Bekannte oder Kolleginnen und Kollegen. Es handelt sich meist um Falschmeldungen (Hoaxes), die dann als Kettenbriefe das Mail-System belasten.
- Wenn Sie ein Mail an viele Empfänger schicken, die untereinander nicht bekannt sind, setzen Sie deren Adressen in „BCC". Damit ist sichergestellt, dass kein Empfänger die E-Mail-Adressen der anderen Adressaten sehen und missbräuchlich verwenden kann.

TIPP:

Nach österreichischer Rechtslage dürfen Sie keine E-Mails an mehr als 50 E-Mail-Empfänger (Massen-E-Mail) oder zu Zwecken der Direktwerbung (Werbe-E-Mail) versenden, sofern Sie nicht vorher deren Zustimmung eingeholt haben. Nähere Informationen zu den rechtlichen Rahmenbedingungen für Aussendungen und Werbe-E-Mails finden Sie auf der Website der Wirtschaftskammer.

PHISHING-MAILS

Phishing ist eine spezielle Form des Social Engineering, bei der es darum geht, Zugangsdaten zu Online-Banking, Online-Zahlungssystemen, Web-Auktionsplattformen etc. zu „ergaunern". Dies geschieht meist in Form von E-Mails, die den Empfängerinnen und Empfängern vorgaukeln, dass aufgrund von Wartungsarbeiten oder Sicherheitsüberprüfungen die Eingabe ihrer Anmeldeinformationen (Login und Passwort bzw. im Bankenbereich PIN und TAN) dringend erforderlich ist. Manchmal wird auch zusätzlich Druck ausgeübt, in dem die Schließung des Zugangs angedroht wird, sollte nicht binnen einer gewissen Frist der Aufforderung entsprochen werden. Ignorieren Sie grundsätzlich alle Mails, die diesem Muster folgen. Die Wahrscheinlichkeit, dass es sich dabei um ein echtes Mail handelt, ist verschwindend gering.

Phishing-Betrüger gehen auch in der zweiten Phase des Betrugs nach einem speziellen Muster vor: Sind sie im Besitz von PIN und TAN, können sie dennoch das Geld nicht einfach auf ihr Konto überweisen, denn das wäre leicht nachvollziehbar. Also werden sogenannte Finanzagenten angeworben, und hier verbirgt sich die zweite Gefahr beim Phishing: Finanzagenten werden über Spam-Mails angeworben, in denen ein Gewinn über einen bestimmten Geldbetrag zugesagt wird. Reagiert ein Mail-Empfänger und gibt seine Kontodaten für die Überweisung bekannt, wird ihm ein Betrag überwiesen, der den Gewinn bei Weitem übersteigt (z.B.: USD 12.305,- statt „gewonnener" USD 123,05). Kurz nach der Überweisung erfolgt wieder eine Kontaktaufnahme, in der auf diesen Fehler hingewiesen wird. Der Empfänger darf dann für die Unannehmlichkeiten einen zusätzlichen Betrag behalten, soll aber den restlichen Differenzbetrag abheben und per internationalem Bargeldtransfer (Western Union, Moneygram, Bitcoin etc.) überweisen. Notfalls wird auch Druck ausgeübt und suggeriert, dass die Versenderin oder der Versender aufgrund dieses Fehlers den Job verlieren könnte. Das gleiche System wird auch angewandt, wenn Sie über ein Online-Auktionshaus eine Ware verkaufen und Ihnen dafür „irrtümlich" ein zu hoher Betrag überwiesen wird.

Aktuelle Browser verfügen über sogenannte Phishing-Filter, die beim Aufruf einer (bereits bekannten) Betrugsseite Alarm schlagen.

Als unwissentlich angeworbener Finanzagent verlieren Sie zwar nicht Ihr eigenes Geld, machen sich aber strafbar und können davon ausgehen, dass Sie zumindest sehr viel Ärger und Unannehmlichkeiten haben werden und möglicherweise sogar regresspflichtig sind. Ignorieren Sie also alle Aufforderungen, „irrtümlich" auf Ihrem Konto geparktes Geld mittels Bargeldtransfer-Services zu versenden. Wenden Sie sich im Zweifelsfall an ihr Bankinstitut.

TIPP:

Phishing-Mails sind oftmals sehr gut gemacht und täuschen selbst Experten. Wenn Sie im Internet nach „Phishing Test" suchen, finden Sie verschiedene Ratgeber, worauf Sie achten müssen, um einen Betrugsversuch zu erkennen. Auf diesen Websites können Sie Ihr Unterscheidungsvermögen auch anhand konkreter E-Mails überprüfen.

GEFÄLSCHTE ABSENDERADRESSEN

Wenn Sie E-Mails bekommen, die von bekannten Absendern stammen, aber unpassende Inhalte enthalten, liegt das oft an einer gefälschten Absenderadresse. Der angezeigte Absendername lässt sich leicht ändern und entspricht oft nicht dem des wirklichen Versenders. Auch Schadprogramme können auf E-Mail-Adressbücher zugreifen und unbemerkt Nachrichten an alle darin gespeicherten E-Mail-Adressen versenden. Als Absender wird häufig der Name einer im Adressbuch gespeicherten Person verwendet.
Sollten Sie darauf angesprochen werden, dass Sie dubiose E-Mails versenden, sollten Sie sofort reagieren: Lassen Sie sich die angeblich von Ihnen versandten Nachrichten vorlegen. Eine Expertin oder ein Experte kann diese prüfen, um zu klären, von wem sie tatsächlich stammen.

SPARSAMER EINSATZ DER EIGENEN MAIL-ADRESSE IM INTERNET

Vorsicht beim Ausfüllen von Webformularen: Häufig führt das Eintragen Ihrer E-Mail-Adresse oder Ihrer persönlichen Daten zu einer Flut von Werbe- bzw. Spam-Mails. Der Handel mit Mail-Adressen wird in verschiedenen Ländern kaum kontrolliert. Prüfen Sie auch hier die Vertrauenswürdigkeit der Website!
Ein guter Ausweg ist es, bei einem Anbieter von Gratis-E-Mail (z.B. http://www.gmx.at, http://www.yahoo.at, http://www.gmail.com, http://www.live.com etc.) einen kostenlosen E-Mail-Account anzulegen, den Sie ausschließlich für derartige Registrierungen verwenden. Damit haben Sie zusätzlich die Möglichkeit, private und geschäftliche E-Mails zu trennen. So können auch Probleme beim Ausscheiden aus dem Unternehmen und der anschließenden Deaktivierung Ihrer E-Mail-Adresse vermieden werden.

5. Gefährliche Schadprogramme

Schadprogramme wie z.B. Computer-Viren enthalten verdeckte Funktionen, die durch Löschen, Überschreiben oder sonstige Veränderungen Schäden an Betriebssystemen, Anwendungsprogrammen und Daten erzeugen. Sie verursachen damit zusätzliche Arbeit und Kosten und haben einen negativen Einfluss auf die Vertraulichkeit, Integrität und Verfügbarkeit von Daten oder Programmen.

WIE KÖNNEN SIE ERKENNEN, DASS IHR PC INFIZIERT IST?

Typische Anzeichen einer Infektion sind:

- Sie können auf bestimmte Laufwerke oder Datenträger nicht mehr zugreifen und Dateien nicht mehr bearbeiten.
- Der Rechner arbeitet mit deutlich reduzierter Leistung (Systemauslastung zumeist auf 100 %), reagiert nicht oder startet in regelmäßigen Abständen neu. Auch der Zugriff auf Dateien dauert länger.
- Der Rechner startet nicht mehr oder benötigt für das Hochfahren deutlich länger.
- Auf dem Bildschirm werden plötzlich unbekannte Meldungen oder Dialogfenster angezeigt.
- Sie erhalten eine E-Mail-Nachricht mit Anhang. Beim Öffnen des Anhangs öffnen und schließen sich verschiedene Dialogfenster und die Systemleistung nimmt sofort deutlich ab.
- Im Internet-Browser sind plötzlich zusätzliche Icons und Symbolleisten sichtbar. Als Startseite erscheint eine Homepage, die Sie nicht eingestellt haben.
- Es werden Warnungen angezeigt, dass bestimmte Programme eine Verbindung mit dem Internet herzustellen versuchen, obwohl dies nicht von Ihnen veranlasst wurde.
- Antiviren- und Antispywareprogramme sind deaktiviert und können nicht neu gestartet werden.
- Ohne Ihr Zutun verschwindet ein Programm von Ihrem Computer.
- Verschiedene Dateien haben plötzlich geänderte Namen. Wenn Sie versuchen, sie zu öffnen, erfahren Sie, dass die Inhalte verschlüsselt wurden und nicht geöffnet werden können.
- Sie können nicht mehr auf bestimmte Dokumente zugreifen. Es erscheint ein Fenster, in dem Sie zur Eingabe eines Codes zum Entschlüsseln der Dokumente aufgefordert werden.
- Manche Viren greifen die zum Starten des Computers erforderlichen Dateien an. Nach dem Einschalten erscheint ein leerer Bildschirm.

Die angeführten Symptome können auch erst nach einer bestimmten Zeit auftreten. Sie können außerdem auch von Hardware- oder Softwarestörungen verursacht werden. Deswegen kann nur eine nähere Untersuchung des Rechners durch eine EDV-Fachkraft Aufschluss über die tatsächlichen Ursachen geben.

RANSOMWARE UND VERSCHLÜSSELUNGSTROJANER

Zu den größten Bedrohungen für Unternehmen im Bereich Internetkriminalität gehört mittlerweile die Ransomware. Die gefährlichsten Vertreter dieser Angriffsvariante sind Verschlüsselungstrojaner, die alle wichtigen Dateien am Computer unlesbar machen. Die Daten werden verschlüsselt; Das Passwort, um sie wieder entschlüsseln zu können, geben die Angreifer erst nach Überweisung eines „Lösegelds“ (engl.: ransom) heraus.

Auch nach Bezahlung ist aber keineswegs sicher, dass die Entschlüsselung funktioniert. Manchmal ist sie in der Schadsoftware gar nicht wirklich vorgesehen oder der Mechanismus zur Entschlüsselung funktioniert nicht. Im schlimmsten Fall sind sowohl die gespeicherten Daten als auch der überwiesene Betrag verloren.

Verschlüsselungstrojaner greifen verschiedene Arten von Dateien an, vor allem Office-Dokumente, Bilder, Video- und MP3-Dateien, manchmal auch E-Mails und Datenbanken. Es handelt sich dabei typischerweise um selbst erstellte und unwiederbringliche Dokumente, die für das Unternehmen sehr wichtig sein können. Im Extremfall kann ein solcher Angriff zum Verlust aller Daten führen!

Um sich gegen Ransomware zu schützen, müssen Sie grundsätzlich die gleichen Verhaltensregeln befolgen wie bei jeder anderen Schadsoftware:

- Prüfen Sie jede E-Mail auf Plausibilität: Ist Ihnen der Absender bekannt und passt der Betreff zum Absender? Gibt es auffällige Rechtschreib- und Grammatikfehler? Haben Sie eine derartige E-Mail erwartet oder kommt sie Ihnen irgendwie verdächtig vor?
- Öffnen Sie keine verdächtigen Dateianhänge! Prüfen Sie zweifelhafte Dateien, indem Sie sie auf eine geeignete Internetseite (z.B. Virustotal.com) hochladen. Wenn Sie den Absender kennen, rufen Sie ihn an und fragen ihn, ob die Nachricht von ihm stammt und worum es sich handelt. Lassen Sie sich nicht von „bedrohlichen" Inhalten (Rechnung, Mahnung etc.) dazu verleiten, eine Datei unbedacht zu öffnen!
- Klicken Sie nie unüberlegt auf Internet-Links in E-Mails! Übertragen Sie den Link mittels „Hyperlink kopieren" in Ihren Browser und prüfen Sie, ob die URL zum Absender passt. Ein Link in einer E-Mail kann zu einer ganz anderen Adresse führen, als in der E-Mail angegeben ist; so etwas ist in jedem Fall als Alarmsignal zu werten.

Zusätzlich sollten Sie noch folgende Punkte beachten:

- Sollte Ihr PC trotz aller Vorsicht mit Ransomware infiziert worden sein, schalten Sie ihn sofort aus – notfalls, indem Sie den Stecker ziehen! Je länger die Schadsoftware Gelegenheit hat, Dateien zu verschlüsseln, desto größer wird der Schaden. Vor der Wiederinbetriebnahme muss der PC daher auf jeden Fall von einer Expertin oder einem Experten geprüft und bereinigt werden.
- Der beste Schutz gegen Ransomware liegt in regelmäßigen und vollständigen Datensicherungen. Übertragen Sie daher alle wichtigen und unwiederbringlichen Daten regelmäßig auf die Serverlaufwerke Ihres Unternehmens oder andere Sicherungsmedien, die Ihnen zu diesem Zweck zur Verfügung gestellt wurden! Wichtige Dateien sollten Sie nie ausschließlich auf Ihrer lokalen Festplatte speichern.

MASSNAHMEN RICHTIG SETZEN

TECHNISCHE SCHUTZMASSNAHMEN

Jeder Rechner mit Internet-Anschluss benötigt Schutz vor Schadsoftware, der regelmäßig aktualisiert werden muss und nicht deaktiviert werden darf:

- Ein Virenschutzprogramm ist unbedingt erforderlich. Die Signatur-Dateien dieser Software müssen täglich aktualisiert werden, da sonst neu entwickelte Computerviren Ihren Computer ungehindert befallen können.
- Alle Betriebssysteme und viele Anwendungsprogramme, insbesondere der Internet-Browser, weisen Sicherheitslücken auf, die erst im Lauf der Zeit entdeckt werden. Ihre Hersteller bieten kostenlose Programmaktualisierungen (Updates oder sog. Hotfixes) an, die diese Fehler ausbessern sollen. Diese Aktualisierungen müssen unbedingt und möglichst ohne zeitliche Verzögerung installiert werden.
- Eine Firewall ist eine Sicherheitsschnittstelle zwischen Ihrem PC und dem Internet und verhindert unerlaubte Zugriffe. Sofern in Ihrem Unternehmen kein zentrales Firewall-System betrieben wird, sollte eine Personal-Firewall auf jedem Arbeitsplatzrechner installiert werden. Diese Firewall darf auf keinen Fall deaktiviert werden.

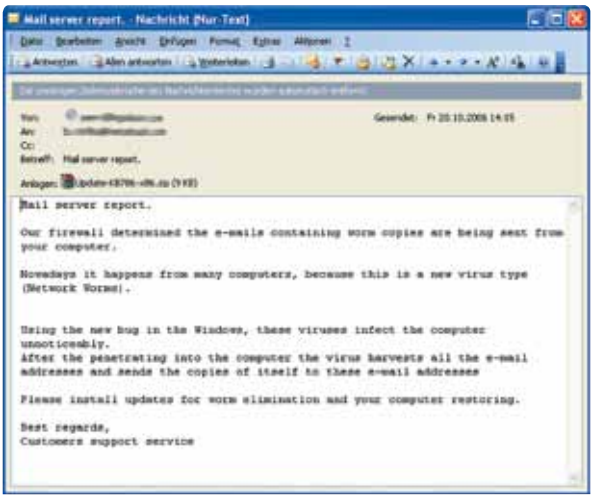
TIPP:

Melden Sie Ihren EDV-Verantwortlichen unverzüglich, wenn Sie Warnhinweise erhalten, dass der Computer ungeschützt ist oder ein Sicherheitsproblem besteht. Vorsicht: Diese Hinweise könnten auch von Schadsoftware stammen. Maßnahmen sollten Sie daher erst nach Rücksprache mit der IT-Abteilung setzen.

MASSNAHMEN BEI DER INTERNET-NUTZUNG

Daten und Programme, die aus dem Internet abgerufen werden, bergen die Gefahr versteckter Schadsoftware in sich. Sie können Benutzerdaten ausspähen, weiterleiten, verändern oder auch löschen. Deswegen:

- Laden Sie Programme nur von vertrauenswürdigen Websites, wie z.B. von den Originalseiten des Software-Herstellers. Dateien, die von Dritten über anonyme Web-Dienste angeboten werden, sind ein Sicherheitsrisiko.
- Daten und Programme von Hackerseiten, Gewinnspielseiten oder anderen dubiosen Homepages sind unbedingt zu meiden. Die Virengefahr ist überdurchschnittlich hoch.
- Überprüfen Sie immer die Größe von Dateien nach einem Download (eventuell wird auch eine Prüfsumme angegeben). Gibt es Abweichungen, besteht die Gefahr unzulässiger Veränderungen – meist durch Viren verursacht. Solche Dateien sollten Sie sofort löschen.
- Heruntergeladene Programme müssen vor ihrer Installation immer mit einem aktuellen Virenschutzprogramm überprüft werden.
- Gepackte (komprimierte) Dateien sollten Sie zuerst entpacken und auf Viren überprüfen. Die Entpackungsprogramme sind so zu konfigurieren, dass die zu entpackende Datei nicht automatisch startet.
- Prüfen Sie bei der Installation neuer Software die Installationsoptionen genau: Viele Programme versuchen, zusätzliche, oft unerwünschte Software zu installieren. Sie können diese Zusatzprogramme bei der Installation abwählen, wenn Sie an der richtigen Stelle eingreifen.


Mail server report. - Nachricht (Nur-Text)

Mail server report.

Our firewall determined the e-mails containing worm copies are being sent from your computer.

Nowadays it happens from many computers, because this is a new virus type (Network Worms).

Using the new bug in the Windows, these viruses infect the computer unnoticeably.
After the penetrating into the computer the virus harvests all the e-mail addresses and sends the copies of itself to these e-mail addresses

Please install updates for worm elimination and your computer restoring.

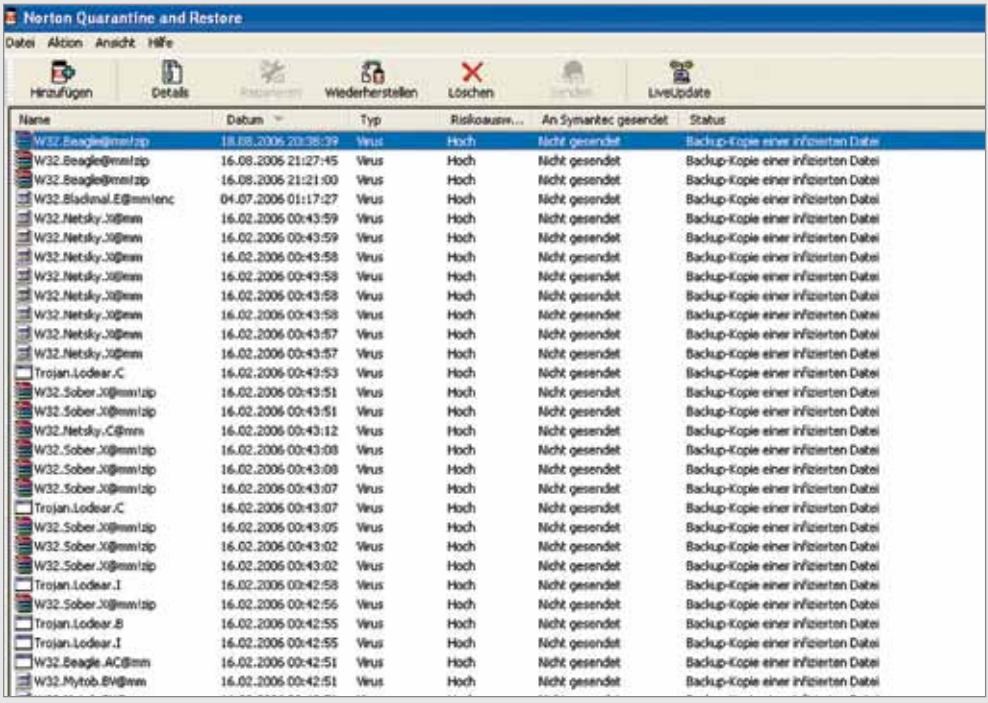
Best regards,
Customers support service

Irreführendes E-Mail: Im Text wird behauptet, dass der Empfänger Viren versenden würde. Tatsächlich wird mit dem Dateianhang der Wurm „Stration.C" übertragen.

VIRENINFEKTION: WAS TUN?

Meist ist die Gefahr schon beseitigt, wenn der Computer Sie auf einen Virus oder ein anderes Schadprogramm aufmerksam macht. In diesem Fall ist der Virus bereits gelöscht oder isoliert bzw. unter Quarantäne gestellt. Dennoch sollten Sie Ihre EDV-Verantwortlichen oder Vorgesetzten darüber informieren.

Wenn allerdings Ihr System das Problem nicht beseitigen kann oder der Verdacht einer Infektion besteht: Speichern Sie Ihre offenen Dateien ab und wenden Sie sich sofort an die zuständigen EDV-Verantwortlichen.



Auszug aus der Quarantäne-Liste eines Privat-Rechners

WAS TUN, WENN KEINE KOMPETENTE IT-FACHKRAFT ERREICHBAR IST?

- Speichern Sie Ihre offenen Dateien und schalten Sie den Rechner ab.
- Überprüfen Sie, ob die Rechner Ihrer Kolleginnen und Kollegen ähnliche Symptome zeigen.
- Recherchieren Sie von einem nicht befallenen Rechner aus im Internet. Verschiedene Websites, insbesondere von Herstellern von Antivirus-Software, enthalten Beschreibungen, wie Sie bestimmte Viren erkennen und entfernen können.
- Verschiedene Antivirus-Programme enthalten bootfähige CDs. Mit diesen kann der befallene PC gefahrlos gestartet und auf Virenbefall geprüft werden. CDs mit derartigen Funktionen können auch aus dem Internet geladen und selbst gebrannt werden, das muss aber auf einem nicht befallenen Rechner erfolgen.
- Verschiedene Websites bieten Online-Virenprüfungen an. Bei Verdacht einer Infektion, d.h. wenn nicht währenddessen konkrete Schäden zu befürchten sind, kann der vermeintlich befallene PC getestet werden.

6. Glossar


1234546521.576232123223152
002455026
01547893468
00245502687
001
2146
3200
2142
1024
14441
0123412

BEGRIFFSERLÄUTERUNGEN:

- Als **AKTIVE INHALTE** werden bestimmte Funktionen von Websites bezeichnet, die die Bedienung einfacher, attraktiver oder bequemer machen sollen. Gemeinsam ist allen diesen Funktionen, dass sie am eigenen PC ausgeführt werden und nicht direkt sichtbar sind. Typische Beispiele für solche aktiven Inhalte sind Java-Applets, JavaScript, VBScript und ActiveX-Controls. Aktive Inhalte sind in der Standardeinstellung der Internet-Browser meistens aktiviert, da ohne sie die Bedienung vieler Websites nicht vollständig funktioniert. Sie stellen aber ein hohes Sicherheitsrisiko dar, da es mit ihrer Hilfe u.a. möglich ist, Schadprogramme zu installieren oder Daten aus dem PC auszulesen und an unbefugte Empfänger zu übertragen.

- **COOKIES** werden eingesetzt, um Informationen zu früher aufgerufenen Websites in kleinen Dateien auf dem Computer zu speichern. Sie ermöglichen beispielsweise, persönliche Einstellungen aus früheren Sitzungen wiederherzustellen oder Informationen aus Online-Shops ohne explizite Benutzeranmeldung zu speichern. Im Allgemeinen sind Cookies ungefährlich, allerdings können sie dazu verwendet werden, das individuelle Surfverhalten auszuforschen und so für zielgruppengerechte Werbung genutzt werden.

- **DIALER** sind Schadprogramme, die eine Telefonverbindung über kostenpflichtige Mehrwertnummern aufbauen. Die Kosten für die Dialer-Verbindung betragen dabei mehrere Euro pro Minute. Die Aktivierung eines Dialers erfolgt in der Regel durch den User selbst, der dem Download oder der Installation eines Programms zustimmt. Davon betroffen sind insbesondere ungeschützte Smartphones.

- **DIGITALE ZERTIFIKATE** bilden die Grundlage für die Authentifizierung von Webservern beim Einsatz von HTTPS. Sie werden außerdem auch zur Verschlüsselung und zum Signieren von E-Mails genützt. Zertifikate werden von einer Zertifizierungsstelle herausgegeben und weisen die Identität des Zertifikatsinhabers aus. Diese Zertifizierungsstellen können wieder durch andere Stellen zertifiziert sein; insgesamt bildet sich so eine Zertifizierungskette oder Zertifikatshierarchie, die bis zu einer obersten Stammzertifizierungsstelle reicht.

- **FTP** ist die Abkürzung für File Transfer Protocol, ein Verfahren zur Übertragung von Dateien zwischen Kommunikationspartnern. Die Datenübertragung ist in beide Richtungen möglich, mittels FTP-Client können Daten vom Server zum Client oder vom Client zum Server übertragen werden. Ähnlich wie bei HTTP werden dabei die Daten (auch Passwörter) unverschlüsselt übertragen. In Zusammenhang mit dem Internet wird FTP vor allem dazu verwendet, Softwareinstallationsdateien von FTP-Servern auf Clients zu übertragen oder neue Webseiteninhalte auf Servern einzuspielen.

- Als **HOAXES** bezeichnet man Warnungen über angebliche neue Computer-Viren, sensationelle Einkunftsmöglichkeiten und dergleichen, die in der Regel über E-Mail verbreitet werden und die Empfänger zur Weiterleitung an Andere auffordern. Bei diesen Warnungen handelt es sich in der Regel um Falschmeldungen oder Kettenbriefe, die verunsichern oder zu unüberlegten Handlungen verleiten sollen. Hoax-Mails und Kettenbriefe sollten daher am besten sofort gelöscht und keinesfalls weitergeleitet werden. Nähere Informationen sind auf der Hoax-Liste der TU-Berlin unter http://hoax-info.tubit.tu-berlin.de/hoax/hoaxlist.shtml zu finden.

- **HTTP** ist die Abkürzung für HyperText Transfer Protocol, dem typischen Übertragungsprotokoll für Webseiten. Über HTTP werden Webseiten, d.h. Texte und Bilder von Servern im Internet an den jeweiligen Browser übertragen. Es können aber auch in Gegenrichtung Daten vom Browser an den Server gesendet werden, z.B. um eine Suchanfrage oder Daten in einem Webformular zur weiteren Verarbeitung an den Webserver zu schicken. HTTP ist ein relativ unsicheres Protokoll, das Daten unverschlüsselt überträgt und keinen Schutz vor dem Abfangen oder Umleiten von Daten bietet. Zur Übermittlung sensibler Daten ist es daher nicht geeignet.

- **HTTPS** ist die Abkürzung für HyperText Transfer Protocol Secure, das durch die Verwendung des Verschlüsselungsprotokolls SSL/TLS ausreichende Sicherheit für die Übertragung sensibler Daten bietet. Mit Hilfe dieses Protokolls werden einerseits die übertragenen Daten verschlüsselt und abhörsicher gemacht, andererseits wird durch die Verwendung von digitalen Zertifikaten die Identität des Webservers gesichert. Angreifern sollte es daher – die richtige Handhabung vorausgesetzt – nicht möglich sein, sich z.B. als E-Banking-Server auszugeben, um Internet-Usern Passwörter, PINs oder TANs zu entlocken.

- **PHISHING** ist ein Kunstwort aus den beiden Begriffen „Password“ und „Fishing“ und bezeichnet den Versuch mittels gefälschter E-Mails an fremde Nutzerdaten (Login, Passwort, TAN etc.) zu gelangen. Normalerweise werden die Empfänger solcher Mails unter Vorspiegelung falscher Tatsachen (Userdaten gingen verloren, Neuidentifikation ist notwendig, ...) aufgefordert, die Webseite einer Bank (Online Shop, Kreditkarteninstitut, Auktionshaus etc.) aufzusuchen und dort ihre Zugangsberechtigungen einzutippen. Diese Webseiten sind ebenfalls gefälscht und sehen den Originalen zum Verwechseln ähnlich.

Die dort eingetippten Daten landen natürlich nicht bei der eigenen Bank, sondern auf den Servern von Betrügern, die dann mit den Nutzerdaten Transaktionen zum Schaden der User durchführen. Grundsätzlich fordert kein seriöses Unternehmen seine Kunden auf, seine Userdaten über das Internet zu bestätigen. Es sind also alle diesbezüglichen Mails zu ignorieren. In Zweifelsfällen sollte man sich telefonisch mit dem (vermeintlichen) Absender in Verbindung setzen.

- Als **ROOTKIT** bezeichnet man Software bzw. eine Softwaretechnik, mit der ein System manipuliert werden kann, sodass bestimmte Dateien, Prozesse, Netzwerkverbindungen, Speicherbereiche nicht mehr angezeigt werden. Damit ist es möglich, das Rootkit und verborgene Schadsoftware einerseits vor Virenscannern und andererseits vor den Computer-Anwenderinnen und -Anwendern zu verstecken.

- **SOZIALE NETZWERKE** sind Netzgemeinschaften, die meist über Internetportale zugänglich sind. Über das Portal können Mitglieder eigene Inhalte erstellen und austauschen. Typische soziale Netzwerke bieten ihren Mitgliedern die Möglichkeit, Profile über die eigene Person, Vorlieben und Interessen anzulegen sowie Kontakte zu Anderen herzustellen und mit diesen zu kommunizieren.

- Als **SPAM** bezeichnet man unerwünschte Werbemails, die mittlerweile rund 90 Prozent des gesamten E-Mail-Verkehrs ausmachen. Auch bei kleineren Unternehmen ist es durchaus möglich, mehrere hundert Spam-Mails pro Tag zu erhalten. Gefährlich ist Spam grundsätzlich nicht, allerdings geht beim Löschen der Werbe-Mails wertvolle Arbeitszeit verloren. Mittels spezieller Spam-Filter können entweder bereits auf Provider-/Mailserver-Ebene oder auch erst am eigenen Rechner unerwünschte Mails gefiltert und gelöscht werden.

- Als **SPYWARE** bezeichnet man Programme, die die User und/oder ihr Surfverhalten ohne deren Wissen ausspionieren. Diese Daten werden an den Hersteller der Software oder auch an Dritte, meist mit dem Zweck, personalisierte Werbung und Pop-ups einzublenden, weitergeleitet. Mittels Spyware können aber auch sensible persönliche Daten an Unbefugte übertragen werden.

- **TROJANISCHE PFERDE (TROJANER)** sind selbständige Programme mit verdeckter Schadensfunktion, ohne Selbstreproduktion. Trojanische Pferde dienen vor allem dazu, Computer auszuspionieren. Der Trojaner verdankt seinen Namen dem Umstand, dass die Schadensroutinen oft in scheinbar nützlichen Programmen versteckt sind. Ein Programm, das zum Zweck der Viren-Entfernung aus dem Internet heruntergeladen wird, kann unter Umständen genau das Gegenteil bewirken. Es ist daher immer auch notwendig, die Seriosität der Quelle, von der man Programme bezieht, zu überprüfen.
-
- **URL** ist die Abkürzung für Uniform Resource Locator, sie ist gewissermaßen die Adressangabe für einen Dienst in einem Computernetzwerk. Die URL für die Website von it-safe ist z.B. http://www.it-safe.at. Eine URL besteht aus der Zugriffsmethode auf diesen Dienst – im Web üblicherweise http oder https, für Datenübertragungen auch ftp – und dem Ort des Dienstes. An die URL kann noch, durch ein Fragezeichen getrennt, ein weiterer Textteil angeschlossen werden, um z.B. eine Anfrage an den verarbeitenden Server zu übertragen.

- **VIREN** sind nicht-selbständige, in andere Programme oder Dateien eingebettete Programmroutinen, die sich selbst reproduzieren und dadurch von Anwenderinnen und Anwendern nicht kontrollierbare Manipulationen in Systembereichen, an anderen Programmen oder deren Umgebung vornehmen.

- **WÜRMER** sind selbständige, selbstreproduzierende Programme, die sich in einem System (vor allem in Netzen) ausbreiten. Zu diesem Zweck verwenden viele Würmer das Adressbuch des infizierten Rechners und versenden Mails mit gefälschten Absenderadressen. Das Öffnen solcher Mails kann bei einem ungeschützten System zu einer Infektion führen.

IST IHR BETRIEB IT-SAFE?

it-safe.at

Jetzt kostenlos herausfinden:
Mit den Online-Ratgebern auf www.it-safe.at

IT-Sicherheit ist für jedes Unternehmen überlebenswichtig!

Mit der Initiative „it-safe.at“ bietet die WKÖ vor allem kleinen und mittleren Unternehmen (KMU) sowie Ein-Personen-Unternehmen (EPU) Hilfestellung:

- Online-Ratgeber it-safe
- Online-Ratgeber Datensicherung
- EPU-Checkliste
- Sicherheits-Handbücher
- News und Tipps im it-safe Blog

Gemeinsam gehen wir’s an und machen auch Ihr Unternehmen IT-sicher: **www.it-safe.at**

bmwfw
Bundesministerium für Wissenschaft, Forschung und Wirtschaft

Der Online-Ratgeber it-safe ist ein gemeinsames Service von BMWFW und WKÖ.

WKO
WIRTSCHAFTSKAMMER ÖSTERREICH