Begleitmaterial zum Vortrag „Sicherheit im Netz“

Computerviren
Viren sind die ältesten Schadprogramme. Sie können sich nur in einem Computer verbreiten. Um auf andere PCs zu gelangen, brauchen sie die „Hilfe“ des Computerbenutzers: Der muss eine vireninfizierte Datei weitergeben.

Würmer
Technisch gesehen sind Würmer Nachfolger der Viren. Sie können sich selbständig über Netzwerk- und Internetverbindungen von einem Computer zum anderen verbreiten (zum Beispiel per E-Mail). Deshalb treten sie inzwischen deutlich häufiger auf und richten mehr Schaden an als Viren.

Trojaner
Diese Schädlinge tarnen sich als nützliche Hilfsprogramme. In ihnen stecken aber gut getarnte Schadprogramme. Trojaner werden in der Regel vom Computerbesitzer selbst auf den PC überspielt, oft in dem Glauben, eine gute Software im Internet kostenlos ergattert zu haben.

Spionage-Programme („Spyware“)
Sie gelangen oft über Trojaner in den Computer. Ihr Auftrag: Daten sammeln und weiterleiten, mit denen andere Zeitgenossen Geld machen können. Sei es, dass Sie auf Grund der von Ihnen besuchten Internetseiten massenhaft Werbung erhalten oder dass Betrüger mit Ihrer Kreditkartennummer einkaufen.

Hintertür-Programme oft per Telefon (Microsoft)
Sie erlauben Computergaunern direkten Zugriff auf den Computer bis hin zur Fernsteuerung. So wurde schon mancher unvorsichtige PC-Benutzer zum Massenversender von Werbe-E-Mails.

Betrügerische E-Mails („Phishing“)
Dies sind keine Schadprogramme, aber höchst gefährlich. Sie gaukeln als Absender etwa Ihre Bank vor und wollen Sie auf fingierte Internetseiten locken. Dort sollen Sie Ihre Konto-Zugangsdaten angeben. Mit den Daten wird dann Ihr Bankkonto geplündert.

Informationen zum sicheren Umgang mit der Email.

Bundesamt
für Sicherheit in der
Informationstechnik

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Onlinekommunikation/E-Mail-Sicherheit/e-mail-sicherheit_node.html

1. Geben Sie niemals Ihre Zugangsdaten am Telefon oder per E-Mail weiter

Ein Anruf oder eine E-Mail ist angeblich von Ihrer Bank und verlangt – oft zur Freischaltung des Kontos nach angeblich technischen Problemen – Ihre IBAN und Passwörter. Eine Bank fragt niemals außerhalb der regulären Online-Transaktionen Ihre Zugangsnummer, eine Geheimzahl (PIN) oder Transaktionsnummer (TAN) ab. Auch beim Telefonbanking geben Sie bitte Ihre IBAN und Geheimzahl nur an, wenn Sie Ihre Bank angerufen haben. Melden sich angebliche Bankangestellte bei Ihnen und verlangt diese Daten, sagen Sie nichts. Stattdessen rufen Sie einfach unter der offiziellen Telefonnummer der Bank zurück und fragen nach.

2. Öffnen Sie keine Links oder Dateianhänge aus E-Mails heraus

Phishing-Mails enthalten oft einen Link auf eine gefälschte Internetseite, die bei der Eingabe Ihre Zugangsdaten ausliest. Leider sieht diese Fälschung der Originalseite oft täuschend ähnlich. Am besten rufen Sie Ihr Online-Banking immer direkt durch das Eintippen der URL in der Browserzeile auf.

3. Enttarnen Sie Phishing-Mails mit dem "Mouse-Over-Effekt"

Eine Mail kommt Ihnen komisch vor? Manchmal hilft es schon, den Mauszeiger über den Links in der Mail zu platzieren. In der Statusleiste des Mail-Clients oder des Webmailers erscheint beim Mouse-Over nämlich die Seite, zu der der Link führt. Sieht dieser Link nicht nach der Originalseite aus und hat darüber hinaus keine HTTPS-verschlüsselte Verbindung, fragen Sie sicherheitshalber beim angeblich absendenden Unternehmen der E-Mail noch mal nach.

4. Starke Passwörter verwenden

Den Zugang zur Banking-Software auf dem Rechner sollten Sie mit einem Passwort sichern, das nur schwer zu knacken ist. Damit Ihre Passwörter besonders sicher sind, verwenden Sie eine Mischung aus Zeichen, Sonderzeichen, Zahlen und Buchstaben und vermeiden Sie Wiederholungen, Zahlenreihen oder bekannte Namen. Und auch ein gutes Passwort wird unsicher, wenn Sie es unverschlüsselt auf Ihrer Festplatte oder sogar im Adress- oder Telefonbuch speichern.

5. Loggen Sie sich nicht über ein öffentliches WLAN in Ihr Online-Banking ein

Sie wissen nämlich nicht, ob und wenn ja wie gut Ihre Daten in so einem WLAN gesichert sind. Nutzen Sie für das Banking unterwegs wenn möglich lieber die LTE-Verbindung Ihres Mobilfunkanbietenden – oder warten Sie, bis Sie in einem gesicherten Netz surfen können.

6. Aktualisieren Sie Browser und System regelmäßig

Halten Sie sowohl Ihr Betriebssystem als auch Ihren Browser immer auf dem neuesten Stand. Damit minimieren Sie die Gefahr von Sicherheitslücken. Generell empfehlen wir auch, ein Virenschutzprogramm zu nutzen und aktuell zu halten.

7. Öffnen sie Emails immer im Reintext Format.

Damit in ihrem Emailprogramm keine schädlichen Anhänge automatisch geöffnet werden können, sollten sie die Einstellung „öffnen im Reintext“ aktivieren und nur bei Bedarf im html Format öffnen.

8. Benutzen sie einen Passwortmanager

Passwort-Manager sind Programme, die dabei helfen, Benutzernamen und verschiedene Passwörter zu verwalten. Mittels Verschlüsselung und eines komplexen Masterpassworts verwahren Passwort-Manager Ihre Passwörter. Sie funktionieren ähnlich wie ein Notizbuch, das in einer Schublade eingeschlossen ist und dessen Inhalte somit nur für die Besitzerin oder den Besitzer einsehbar sind. Der Vorteil liegt auf der Hand: Anstelle von vielen verschiedenen Passwörtern muss sich nur noch eins gemerkt werden. Verliert man allerdings dieses Masterpassworts, sind im schlechtesten Fall alle Daten verloren.

9. Datensicherung

Wie sichere ich meine daten? Die häufig genutzten Methoden zur Datensicherung.Es gibt verschiedene Methoden, um die Daten von Ihrem Laptop oder PC zu sichern. Im Folgenden stellen wir Ihnen die gängigsten und effektivsten Methoden vor.

a. Externe Festplatte als Backup-Lösung

Eine externe Festplatte ist eine der einfachsten und zuverlässigsten Methoden, um Ihre Daten zu sichern. Sie ist tragbar und bietet viel Speicherplatz für Ihre wichtigen Dateien. Um mit einer externen Festplatte zu arbeiten, schließen Sie diese einfach über ein USB-Kabel an Ihren Laptop oder PC an. Sobald die Festplatte verbunden ist, können Sie die gewünschten Dateien und Ordner einfach per Drag & Drop darauf kopieren.Es ist ratsam, Ihre externe Festplatte regelmäßig zu überprüfen und sicherzustellen, dass sie in gutem Zustand ist. Sie können auch mehrere externe Festplatten verwenden, um zusätzliche Sicherheit und Redundanz zu gewährleisten. Eine externe Festplatte ist nicht nur erschwinglich, sondern auch eine effektive Lösung für Ihre Datensicherungsbedürfnisse**.**

HDD und SSD-Festplatte im Backup-Vergleich

Wenn es um die Auswahl des richtigen Speichermediums für Ihre Datensicherung geht, stehen Ihnen hauptsächlich zwei Optionen zur Verfügung: HDDs (Festplattenlaufwerke) und SSDs (Solid State Drives). Beide Typen haben ihre eigenen Vor- und Nachteile, die bei der Entscheidung berücksichtigt werden sollten.

HDDs (Festplattenlaufwerke) sind die traditionelle Art der Datenspeicherung. Sie verwenden bewegliche Teile, um Daten auf magnetischen Platten zu speichern. Dies macht sie im Allgemeinen günstiger und bietet mehr Speicherplatz für Ihr Geld. Wenn Sie eine große Menge an Daten sichern möchten, kann eine HDD eine kosteneffiziente Lösung sein.Zudem sind sie in der Lage, große Datenmengen schnell zu speichern und abzurufen. Allerdings sind sie auch anfälliger für physische Beschädigungen und mechanische Ausfälle, da die beweglichen Teile während des Betriebs Schaden nehmen können.

SSD (Solid State Drives) hingegen verwenden Flash-Speicher und haben keine beweglichen Teile. Dadurch sind sie nicht nur schneller in der Datenspeicherung und -abfrage, sondern auch robuster und widerstandsfähiger gegenüber physikalischen Schäden. Die Zugriffsgeschwindigkeit von SSDs kann die Sicherung und Wiederherstellung Ihrer Daten erheblich beschleunigen, was besonders wichtig ist, wenn Sie regelmäßig große Datenmengen übertragen müssen. Allerdings sind SSDs in der Regel teurer pro Gigabyte Speicherplatz, was bei der Kaufentscheidung zu beachten ist.

b. Datensicherung auf einem Cloud-Speicher

Die Nutzung eines Cloud-Speichers ist eine moderne und praktische Möglichkeit, um Ihre Daten zu sichern. Bei dieser Methode werden Ihre Dateien auf Servern im Internet gespeichert, statt auf physischen Geräten wie externen Festplatten. Das bedeutet, dass Sie von überall auf Ihre Daten zugreifen können, solange Sie eine Internetverbindung haben. Cloud-Anbieter wie Google Drive, Dropbox oder Microsoft OneDrive bieten verschiedene Speicherplatzoptionen, die sich leicht an Ihre Bedürfnisse anpassen lassen.

c. Datensicherung auf einem NAS

Ein NAS (Network Attached Storage) ist eine spezialisierte Speicherlösung, die eine hervorragende Möglichkeit zur Datensicherung bietet. Es handelt sich um ein Gerät, das an Ihr Netzwerk angeschlossen wird und mehrere Festplatten enthalten kann, wodurch eine hohe Speicherkapazität und Redundanz gewährleistet wird. Ein NAS bietet den Vorteil, dass mehrere Benutzer gleichzeitig auf die gespeicherten Daten zugreifen können, was es ideal für kleine Büros oder Familien macht.

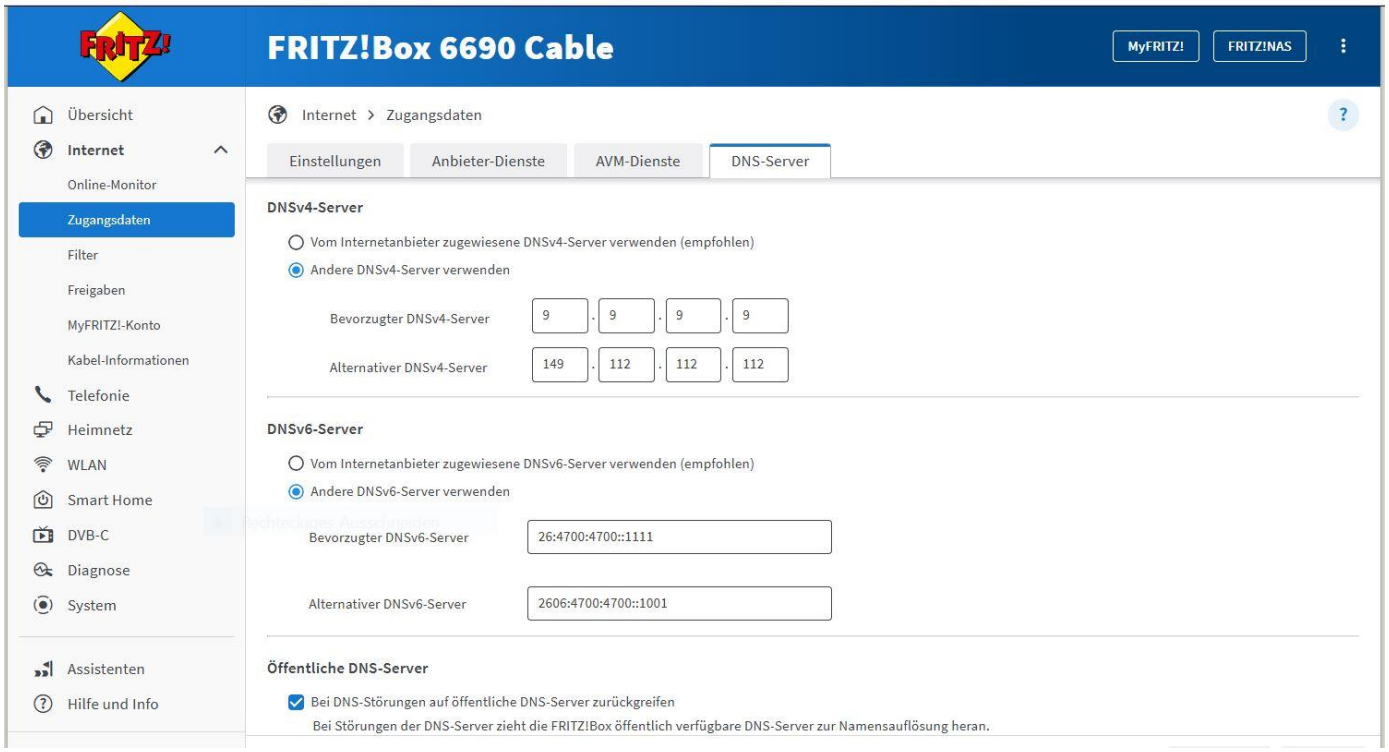
d. Datensicherung mit einem USB-Stick

Die Verwendung eines USB-Sticks zur Datensicherung kann auf den ersten Blick eine praktische Lösung erscheinen, da diese Geräte klein, tragbar und einfach zu verwenden sind. Man kann Dateien einfach per Drag & Drop auf den Stick übertragen und ihn dann sicher verstauen oder sogar unterwegs einsetzen. Allerdings bringt diese Methode auch einige Nachteile mit sich, die es wichtig machen, ihre Verwendung abzuwägen.

USB-Sticks sind anfällig für Verlust oder Beschädigung, insbesondere wenn sie häufig transportiert werden. Zudem besteht die Gefahr von Datenkorruption, insbesondere wenn der USB-Stick nicht ordnungsgemäß entfernt wird oder bei plötzlichen Stromausfällen. Ein weiterer Nachteil ist die begrenzte Speicherkapazität, die im Vergleich zu externen Festplatten oder Cloud-Speichern oft geringer ist. Während USB-Sticks für kleine Datenmengen funktionieren, wird es schwierig, große Datensicherungen darauf abzulegen.

10. DNS Server

https://www.privacy-handbuch.de/handbuch_93d.htm



Im Smartphone: