Tipps gegen Angriffe aus dem Internet

Kurztipps

- Achten Sie darauf, dass Sie immer die aktuellen Sicherheitsupdates des Herstellers installiert haben, und zwar für das Betriebssystem und alle installierten Programme, allen voran u.a. Web-Browser, Office, Flash Player, Adobe Reader. Am besten nutzen Sie dafür die in den meisten Programmen vorhandene Funktion „Automatische Updates“.
- Aktualisieren Sie Ihr Virenschutzprogramm regelmäßig, die Signaturdatenbanken mindestens täglich. Nutzen Sie dafür am besten die eingebaute Funktion „Automatische Updates“.
- Als Angehöriger der TU Clausthal können Sie das bereit gestellte Programm verwenden: Sophos.
- Nutzen Sie die in Ihrem Betriebssystem enthaltene Personal Firewall – und Seien Sie vorsichtig, welche Zugriffe Sie dann auf Anfrage erlauben. Die Personal Firewall schützt in gewissem Rahmen vor Angriffen von außen und überprüft auch (sofern Sie es nicht manuell freigeben oder die Überprüfung ausschalten!) die Daten, die von Ihrem Rechner ggf. unbemerkt gesendet werden.
- Verwenden Sie ausschließlich ein Benutzerkonto mit eingeschränkten Rechten zum Internetzugriff, sei es per Browser oder E-Mail oder sonstigem – niemals ein Konto mit Administratorrechten! Wie Sie ein einfaches Benutzerkonto ohne Administratorrechte einrichten, erklärt das Bundesamt für Sicherheit in der Informationstechnik hier: Microsoft Windows, Mac OS X, Linux Ubuntu.
- Bleiben Sie misstrauisch und halten Sie sich bei der Weitergabe persönlicher Informationen zurück. Denken Sie nach, bevor Sie einen Link anklicken, einen Dateianhang öffnen oder ein Formular ausfüllen. Fragen Sie bei einer E-Mail im Zweifel telefonisch nach, ob der Absender der Mail authentisch ist. Laden Sie Software möglichst ausschließlich von der Seite des Herstellers direkt herunter, oder von wirklich vertrauenswürdigen Verteilern wie https://www.heise.de/download/

Ergänzende Tipps

- Nutzen Sie einen modernen Browser, der moderne Sicherheitstechnologien verwendet, etwa eine Sandbox. Chrome setzt dieses Konzept beispielsweise konsequent um. Darüber hinaus sollte der Browser einen Filter besitzen, der sie vor gefährlichen Seiten warnt, bevor Sie die Seite wirklich aufrufen (URL Check). Beispiele sind der Smart Screen Filter beim Internet Explorer sowie der Phishing- und Malwareschutz bei Google Chrome und Mozilla Firefox. Allerdings können diese Filter teilweise „nach Hause telefonieren“, also die zu prüfenden Adressen an den Hersteller melden. Verwenden außerdem Sie nur so wenige Plugins wie wirklich nötig. Manche Plugins allerdings sind hilfreich für sichereres Surfen: https://www.secuso.informatik.tu-darmstadt.de/de/secuso/ Weitere Empfehlungen zur sicheren Konfiguration Ihres Browsers hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) für Sie zusammengestellt:

Dieses Dokument stammt aus der Dokuwiki-Instanz mit dem Titel RZ-Dokumentationen, die vom Rechenzentrum der Technischen Universität Clausthal bereitgestellt wird.

https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/EinrichtungSoftware/EinrichtungBrowser/derbrowser_node.html

- Verwenden Sie sichere Passwörter. Benutzen Sie für jeden genutzten Online-Dienst – wie E-Mail, Online Shops, Online Banking, Foren, Soziale Netzwerke – jeweils ein anderes, sicheres Passwort und ändern Sie diese Passwörter auch regelmäßig. Voreingestellte Passwörter eines Herstellers oder Anbieters sollten Sie sofort ändern. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat Hilfestellungen für ein sicheres Passwort bereit gestellt: https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html. Einige Online-Demonstrationsseiten geben Ihnen einen ganz groben Eindruck von der Sicherheit eines Passworts, beispielsweise hier: https://password.kaspersky.com/de/
- Achten Sie darauf, dass sie ausschließlich verschlüsselte Verbindungen nutzen, um persönliche Daten zu übertragen, etwa beim Online Banking, beim Einkaufen oder auch bei jeder Passwort-Eingabe. Jeder seriöse Online-Dienst bietet eine Verschlüsselung an, meist durch die Nutzung des sicheren Kommunikationsprotokolls „HTTPS“. Erkennen können Sie dies an der Internetadresse, die bei Verschlüsselung mit „https:“ beginnt statt „http:“. Außerdem zeigt Ihr Browser ein kleines Schlosssymbol an.
- Räumen Sie auf! Nicht benötigte Programme sollten Sie deinstallieren. Was gar nicht drauf ist auf Ihrem Rechner, kann auch nicht angegriffen werden oder sonstige Fehler verursachen.
- Sichern Sie Ihre Daten! Fertigen Sie Sicherheitskopien und Backups von Ihren Daten an, im einfachsten Fall auf einer externen Festplatte, die aber nicht ständig als „Laufwerk“ verbunden sein darf. Institute und Einrichtungen der TU Clausthal sollten den vom RZ angebotenen Backup- und Archiv-Service nutzen https://doku.tu-clausthal.de/doku.php?id=netvault_backupsystem:start.
- Nutzen Sie ausschließlich verschlüsselte WLANs (mindestens WPA2 als Standard, keinesfalls unverschlüsselt oder WEP) Wenn Sie ein WLAN („Wireless LAN“, drahtloses Netzwerk). Wie Sie zu Hause ein sicheres WLAN einrichten können, erklärt das Bundesamt für Sicherheit in der Informationstechnik (BSI) hier: https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/EinrichtungWLAN-LAN/EinrichtungLAN-WLAN_node.html - auf dem Gelände der TU Clausthal können Angehörige der TU das vom RZ bereit gestellte WLAN „eduroam“ nutzen: https://doku.tu-clausthal.de/doku.php?id=campus-wlan_wituc_eduroam
- Eine Möglichkeit, den Sicherheitsstatus Ihres Computers zu überprüfen, bietet die Initiative botfrei des eco-Verbands: https://www.check-and-secure.com/start/

Weitere Informationen

- Zu Fragen der IT-Sicherheit hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) umfangreiche Tipps und Checklisten veröffentlicht: Tipps und Checklisten
- Für einen Schnelltest eignet sich Avira PC-Cleaner – aber natürlich ersetzt die Software keinen vollwertigen Virenscanner.
- Weitere Tools finden sich bei Heise Download
- Siehe auch https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Checklisten/Massnahmen_gegen_Internetangriffe.html

Dieses Dokument stammt aus der Dokuwiki-Instanz mit dem Titel RZ-Dokumentationen, die vom Rechenzentrum der Technischen Universität Clausthal bereitgestellt wird.

Phishing-Webseiten

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt jedem Nutzer, das folgende Anti-Phishing Training durchzuführen – dieser Empfehlung kann sich das RZ nur anschließen:

SECUSO Anti-Phishing-Training (online)

In Deutschland hat sich eine interdisziplinäre Vereinigung aus Wissenschaftlern der Ruhr-Universität Bochum des Phishing-Problems angenommen. Die „Arbeitsgruppe Identitätsmissbrauch im Internet“ (A-I3) stellt auf ihrem Online-Portal nicht nur aktuelle Informationen zu Themen der IT-Sicherheit bereit, sondern auch konkrete Hilfestellungen und Tools: https://www.a-i3.org/

[mitarbeitende]

Direkt-Link:
https://doku.tu-clausthal.de/doku.php?id=it-sicherheit:internet:start&rev=1721975948

Letzte Aktualisierung: **06:39 26. July 2024**

Dieses Dokument stammt aus der Dokuwiki-Instanz mit dem Titel RZ-Dokumentationen, die vom Rechenzentrum der Technischen Universität Clausthal bereitgestellt wird.