UNI WÜ RECHENZENTRUM

Verhalten bei IT-Sicherheitsvorfällen

Ruhe bewahren & IT-Vorfall melden

IT-Vorfallnummer

0931 / 31 - 85050

SCAN ME

https://go.uniwue.de/sicherheitsvorfall

Bei der Meldung beachten:

- Wer meldet den Vorfall?
- Welches IT-System ist betroffen?
- Was haben Sie beobachtet?
- Wann ist das Ereignis eingetreten?
- Wo befindet sich das betroffene IT-System? (Raum, Gebäude)

Verhaltenshinweise:

Weiteres Arbeiten am IT-System einstellen

Beobachtungen dokumentieren

Maßnahmen nur nach Anweisung einleiten

11 goldene Regeln zur Erhöhung der IT-Sicherheit

Betriebssystem aktuell halten

Halten Sie Ihr Betriebssystem stets aktuell, indem Sie verfügbare Updates zeitnah einspielen, da bekannte Schwachstellen für automatisierte Angriffe gegen verwundbare Systeme ausgenutzt werden

Virenscanner einsetzen und aktuell halten

Schützen Sie Ihren Rechner vor der Infizierung mit Schadsoftware wie Viren, Würmern und Trojanischen Pferden durch die Nutzung eines Virenscanners. Die bloße Installation einer derartigen Software ist allerdings für einen wirksamen Schutz nicht ausreichend. Entscheidend sind die Aktualität und die richtige Konfiguration der wichtigsten Funktionen des Programms.

Anwendungsprogramme richtig konfigurieren und aktuell halten

Hierzu gehören insbesondere Office-Programme (MS-Office, OpenOffice, Acrobat, …), Internetbrowser und E-Mail-Programme, aber auch Programme zum Chatten oder zum Abspielen von Multimediainhalten (Windows Mediaplayer, Realplayer, Winamp, …).
Durch gezielt manipulierte Webseiten und Dateien ist das Bedrohungspotential hier mittlerweile genauso hoch wie bei Serverdiensten, die Anwendungen werden aber im Gegensatz zu diesen bei einem Betriebssystemupdate nicht mit aktualisiert.

Sichere Passwörter verwenden

Alle Benutzerkonten eines Systems müssen mit einem Passwort versehen sein, da der Rechner sonst leicht über das Netzwerk angreifbar ist. Insbesondere wird bei vielen Standardinstallationen von Windows kein Administratorkennwort gesetzt! Passwörter sollten einige Mindestanforderungen bezüglich Länge und Komplexität erfüllen, damit sie nicht durch einfaches (evtl. automatisiertes) Durchprobieren erraten werden können: https://go.uniwue.de/passwort

Nicht mit Administratorenrechten arbeiten

Sie sollten im Normalfall lokal nicht mit Administratorrechten arbeiten, sondern lediglich mit den eingeschränkten Rechten eines normalen Benutzers. Bei allen modernen Betriebssystemen können Benutzerkonten mit verschiedenen Rechten versehen werden. Einen unbegrenzten Zugriff auf alle Funktionen des Betriebssystems erhalten Benutzerkonten der Kategorie "Administrator" bzw. "root". Bei Konten der Kategorie "Benutzer" bzw. "eingeschränkt" sind die Rechte dagegen limitiert.

Software und Daten aus sicheren Quellen nutzen

Software aus nicht vertrauenswürdigen Quellen (z.B. P2P-Tauschbörsen oder inoffizielle Webseiten) enthält häufig Schadsoftware wie Viren, Würmer, Trojaner und Rootkits. Beim Öffnen bzw. Ausführen der entsprechende Datei(en) wird die Schadsoftware aktiv, vielfach ohne dass der Nutzer dieses bemerkt. Dabei ist es unerheblich, ob es sich um eine manipulierte Anwendung oder um manipulierte Daten für eine verwundbare Anwendung handelt.

Rechner vor unberechtigtem Zugriff schützen

Lassen Sie Ihren Rechner nicht unbeobachtet, wenn Sie angemeldet sind. Loggen Sie sich aus, sperren Sie den Zugriff oder aktivieren Sie einen Bildschirmschoner mit sicherem Passwort, wenn Sie Ihren Arbeitsplatz verlassen, auch wenn es sich nur um eine vermeintlich kurze Zeitspanne handelt.

Keine zweifelhaften Emails bearbeiten oder beantworten

Führen Sie grundsätzlich keine Software aus, die Ihnen als E-Mail-Anhang zugesandt wird. Deaktivieren Sie im E-Mail-Programm die automatische Anzeige bzw. das Ausführen von E-Mail-Anhängen. Misstrauen Sie E-Mails, die die Aufforderung enthalten, Software zu installieren oder Passwörter, Kreditkartennummern, PINs, TANs oder ähnliches zu übermitteln. Antworten Sie nicht auf E-Mails mit unerwünschtem oder zweifelhaftem Inhalt, auch nicht, um die Versendung dieser E-Mails abzubestellen. Virenbefallene E-Mails täuschen in der Regel vertraute Absenderadressen vor.

Sensible Informationen nicht leichtfertig preisgeben

Seien Sie misstrauisch, wenn Sie jemand wegen eines (vermeintlichen) Problems kontaktiert, und von Ihnen sensible Daten wie Passwörter oder Konfigurationseinstellungen wissen möchte. Die IT-Verantwortlichen der Hochschule und externe Dienstanbieter werden Sie nicht nach Ihrem Passwort fragen.
Lassen Sie sich im Zweifelsfall den Namen des IT-Verantwortlichen nennen und rufen Sie Ihn unter der Telefonnummer aus dem Adressbuch bzw. Informationssystem der Hochschule zurück.

Nichtbenötigte Dienste deaktivieren

Entfernen Sie nicht benötigte Dienste und Anwendungsprogramme oder installieren Sie diese erst gar nicht. Falls Dienste/Programme nicht permanent benötigt werden (Chat-Client, …), dann sollten diese manuell gestartet und nach Gebrauch wieder deaktiviert/beendet werden.

Daten/Systeme sichern

Die sorgfältige Anwendung der Goldenen Regeln verbessert die Sicherheit Ihres Systems und der darauf gespeicherten Daten. Ein absolut sicherer Schutz gegen Angriffe, Anwenderfehler oder Hardwareschäden ist leider nicht möglich. Da Dateien im Schadensfall auch verändert werden können, sollte eine Datensicherung auch eine Wiederherstellung zu einem weiter zurückliegenden Zeitpunkt erlauben. Um Datenträgerfehlern vorzubeugen sollten Backups (evtl. rotierend) auf verschiedenen Datenträgern gesichert werden.
Das zentrale Backup des Rechenzentrums sichert die Netzlaufwerke im Novellnetz, den zentralen E-Mail-Server und die Serversysteme des Rechenzentrums.
Lokale Laufwerke Ihres Rechners werden vom zentralen Backup nicht erfasst.