UNI WÜ RECHENZENTRUM

Behavior during IT security incidents

Keep calm & report IT incident

IT incident number

0931 / 31 - 85050

SCAN ME

https://go.uniwue.de/sicherheitsvorfall

Pay attention when reporting:

Who reports the incident?

Which IT-System is affected?

What did you observe?

When did the event occur?

Where is the affected IT system located? (Room, Building)

Behaviour hints:

Stop further work on the IT system

Documenting observations

Take measures only upon instructions

11 golden rules to increase IT security

Keep operating system up to date

Keep your operating system up to date by installing available updates promptly, as known vulnerabilities are exploited for automated attacks against vulnerable systems.

Use a virus scanner and keep it up-to-date

Protect your computer from infection with malware such as viruses, worms and Trojan horses by using a virus scanner. However, the mere installation of such software is not sufficient for effective protection. It is crucial that the most important functions of the program are up-to-date and correctly configured.

Configure application programs correctly and keep them up-to-date

This includes in particular Office programs (MS-Office, OpenOffice, Acrobat, ...), Internet browsers and e-mail programs, but also programs for chatting or playing multimedia content (Windows Mediaplayer, Realplayer, Winamp, ...). Due to deliberately manipulated websites and files, the threat potential here is now just as high as with server services, but unlike these, the applications are not updated when the operating system is updated.

Use secure passwords

All user accounts on a system must be password protected, otherwise the computer is easily attacked over the network. In particular, many standard installations of Windows do not set an administrator password! Passwords should meet some minimum requirements regarding length and complexity so that they cannot be guessed by simple (possibly automated) trial and error:
https://go.uniwue.de/passwort

Do not work with administrator rights

You should not normally work locally with administrator rights, but only with the restricted rights of a normal user. With all modern operating systems, user accounts can be assigned different rights. User accounts of the category "Administrator" or "root" have unlimited access to all functions of the operating system. Accounts of the category "user" or "restricted", however, have limited rights.

Use software and data from secure sources

Software from untrustworthy sources (e.g. P2P file sharing networks or unofficial websites) often contains malware such as viruses, worms, Trojans and rootkits. When opening or executing the corresponding file(s), the malware becomes active, often without the user being aware of it. It is irrelevant whether it is a manipulated application or manipulated data for a vulnerable application.

Protect computers from unauthorized access

Do not leave your computer unattended when you are logged in. Log out, block access or activate a screen saver with a secure password when you leave your workplace, even if it is only for a supposedly short period of time.

Do not edit or answer dubious emails

Never run any software that is sent to you as an email attachment. In your e-mail program, disable the automatic display or execution of e-mail attachments. Distrust e-mails that contain requests to install software or to transmit passwords, credit card numbers, PINs, TANs or similar. Do not reply to e-mails with unsolicited or dubious content, even to cancel the sending of such e-mails. Virus-infected e-mails usually fake familiar sender addresses.

Do not disclose sensitive information lightly

Be suspicious if someone contacts you about a (supposed) problem and wants to know sensitive information like passwords or configuration settings. The university's IT managers and external service providers will not ask you for your password; if in doubt, ask for the name of the IT manager and call him/her back at the telephone number in the university's address book or information system.

Disable unneeded services

Remove unnecessary services and application programs or do not install them at all. If services/applications are not permanently required (chat client, ...), they should be started manually and deactivated/terminated after use.

Back up data/systems

The careful application of the Golden Rules improves the security of your system and the data stored on it. Unfortunately, absolutely secure protection against attacks, user errors or hardware damage is not possible. Since files can also be changed in the event of damage, a data backup should also allow a recovery to a point in time further back in time. In order to prevent data carrier errors, backups (possibly rotating) should be saved on different data carriers. The central backup of the data center secures the network drives in the Novell network, the central e-mail server and the server systems of the data center. Local drives of your computer are not covered by the central backup.

translated by deepl.com