

SENSIBILISIERUNG FÜR INFORMATIONSSICHERHEIT – UMGANG MIT INFORMATIONEN

IT Equipment & Software

| IT EQUIPMENT & SOFTWARE

EINFÜHRUNG



'IT-Equipment & Software'

Das IT-Equipment beschreibt die von uns verwendeten Geräte wie Desktops, Laptops, Tablets, Telefone, USB-Sticks und externe Festplatten.

In diesem Abschnitt erhaltst Du Informationen zum Schutz der IT-Equipment und den darauf gespeicherten Daten, sowohl wie sie vor Verlust, Diebstahl oder Beschädigung geschützt werden können.

Szenarien

Das IT-Equipment beschreibt die von uns verwendeten Geräte wie Desktops, Laptops, Tablets, Telefone, USB-Sticks und externe Festplatten. Sowohl das Gerät als auch die darauf gespeicherten Daten sind für das Unternehmen wertvoll, und den Benutzern muss daher bewusst sein, wie sie vor Verlust, Diebstahl oder Beschädigung geschützt werden können.

Computacenter stellt Dir IT-Equipment zu Verfügung, das Dir die Erledigung Deiner Aufgaben ermöglicht. Es gibt einige einfache Dinge, die Du tun kannst, um Dein Equipment und Daten sicher zu schützen.



Unternehmenseigenes IT-Equipment

Du solltest nur zugelassenes IT-Equipment an das Netzwerk anschließen. Dies verhindert, dass Geräte, die möglicherweise keine geeigneten Sicherheitseinstellungen haben, Malware einzuführen.

Privates IT-Equipment (d. h. im Privatbesitz befindliches, nicht unternehmenseigenes IT-Equipment) darf nicht für geschäftliche Tätigkeiten der Computacenter verwendet werden, es sei denn, dies wurde ausdrücklich genehmigt (z. B. durch GME2). Dies gilt auch für die

Nutzung privater Smartphones, Tablets und PDAs, um Daten zu kopieren und/oder zu speichern.

Verbindungen zum Unternehmensnetzwerk

Schließe nur von Computacenter genehmigtes IT-Equipment an das Unternehmensnetzwerk an. Achte darauf und erinnere bitte externe Besucher daran, Laptops nicht in das Computacenter-Netzwerk einzubinden, insbesondere nicht in Besprechungsräumen.

Für nicht genehmigte IT-Geräte gibt es einen Gast-Wi-Fi-Dienst, mit dem eine Verbindung zum Internet hergestellt werden kann.

Konfiguration

Ändere nicht die Konfiguration des unternehmenseigenen IT-Equipments.

Das IT-Equipment von Computacenter ist darauf ausgelegt, die gesamte IT-Infrastruktur zu schützen. Durch Ändern der Konfiguration können diese Einstellungen deaktiviert werden.

Nicht-standardmäßige Software

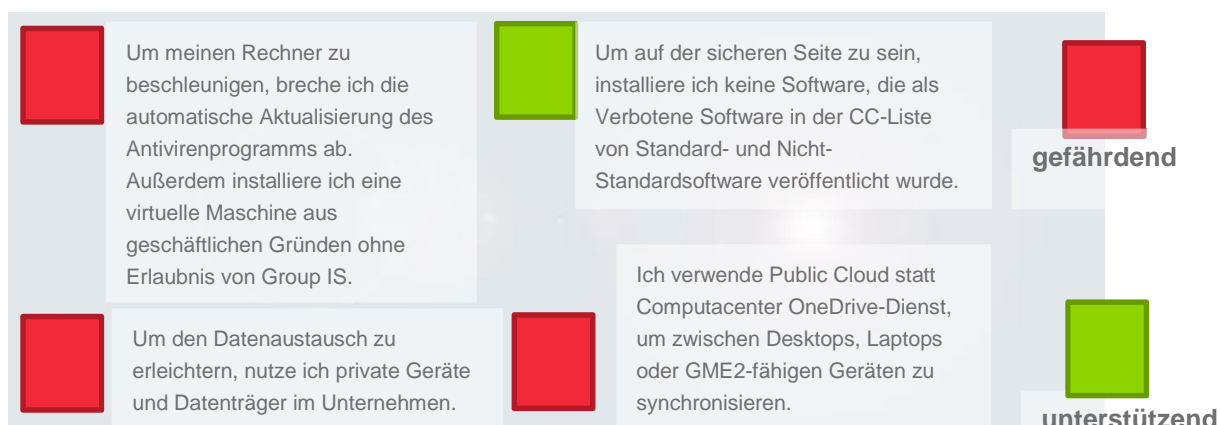
Computacenter stellt Dir Software zu Verfügung, die Dir die Erledigung Deiner Aufgaben ermöglicht. Solltest Du zusätzliche Software benötigen, um bestimmte Geschäftstätigkeiten ausführen zu können, befolge den Genehmigungsprozess für nicht-standardmäßige Software. Nicht genehmigte Software, insbesondere aus dem Internet, kann Malware enthalten.

Schutz vor Verlust oder Diebstahl

Sorge dafür, dass das von Dir verwendete IT-Equipment in gutem Zustand und vor Verlust geschützt ist.

Trage z. B. Geräte in einem geeigneten Schutzgehäuse und lasse sie nie unbeaufsichtigt an öffentlichen Orten liegen. Transportiere Dein Equipment blickgeschützt, also im Kofferraum des Fahrzeugs.

Computacenter IT Equipment schützt und verbessert die gesamte IT-Infrastruktur. Alle technischen Maßnahmen sind wirkungslos, wenn Mitarbeiter sie umgehen oder nicht umsetzen. Was hältst Du von diesen Handlungen? Gefährden sie die Schutzmaßnahmen oder unterstützen sie diese?



Wenn Du Dir die Liste der Standard- und Nicht-Standard-Software ansiehst, weißt Du, was nicht installiert werden darf. Die Liste kann im NGSD-Portal unter der Artikelnummer 180322103411386 eingesehen werden.

Die anderen drei Maßnahmen stellen ein erhebliches Risiko dar und sind daher verboten.

Du kannst die Artikelnummer 180322103411386 kopieren und in das Suchfeld des NGSD-Portals einfügen, um auf diese Liste zuzugreifen.

Zusammenfassung



In diesem Abschnitt hast Du gelernt, dass das IT-Equipment, was wir nutzen und ins Computacenter Netzwerk einbinden...

- muss von Computacenter genehmigt werden,
- muss in gutem Zustand sein und vor Verlust geschützt werden,
- darf nicht geändert werden,
- benötigt vor der Verwendung oder Installation von nicht standardmäßiger Software eine Genehmigung

Datenschutzverletzungen und Informationssicherheitsvorfälle:

Wenn Du glaubst, dass Dein Gerät mit Malware infiziert wurde, melde sofort einen Informationssicherheitsvorfall über NGSD.