Vorlagen

- Copyright
- Copyright CC BY
- [SHORT] Technische und organisatorische Maßnahmen zur Sicherstellung der Verfügbarkeit und der Integrität

Copyright

Copyright CC BY

C
B
Y

[SHORT] Technische und organisatorische Maßnahmen zur Sicherstellung der Verfügbarkeit und der Integrität

Zur Sicherstellung der Verfügbarkeit und der Integrität (Korrektheit) von IT-Systemen sind folgende Maßnahmen erforderlich/sinnvoll:

Maßnahmen zur Absicherung	
Datensicherung	STARK EMPFOHLEN
Sicherstellung der Herstellerunterstützung	STARK EMPFOHLEN
Laufendes Einspielen von kritischen Software Patches / Updates	STARK EMPFOHLEN
Test neuer Software / Software-Versionen	STARK EMPFOHLEN
Migrationsplanung für Versionsumstellungen und Vorsorge durch Rollback-Szenarien	STARK EMPFOHLEN
Vereinbarung von Servicelevels (bei Systemoutsourcing / Cloudservices)	STARK EMPFOHLEN
DDoS-Schutz	STARK EMPFOHLEN
Dokumentation aller (wesentlichen) IT-Systeme	STARK EMPFOHLEN
Erstellung von Notfallplänen für den Ausfall von IT-Systemen	STARK EMPFOHLEN
Überwachung (Monitoring) aller (wesentlichen) IT-Systeme	EMPFOHLEN
Unterbrechungsfreie Stromversorgung (USV) / Notstromversorgung	EMPFOHLEN

Aufstellung der zentralen Hardwarekomponenten in geeigneten (Rechner)Räumen	EMPFOHLEN
redundante Gestaltung kritischer Hardwarekomponenten	EMPFOHLEN
örtlich getrennter Ausweich-Rechnerraum	OPTIONAL
redundante Netzwerkverbindungen	OPTIONAL
Vereinbarung einer (notariellen) System- / Sourcecodehinterlegung für wesentliche IT-Systeme	OPTIONAL

Datensicherung [STARK EMPFOHLEN]

> **Ziele/Nutzen**: Die Sicherung von Daten und Programmen dient zur Vorsorge vor dem Verlust oder einer nicht gewollten Manipulation von Programmen oder Daten infolge von Hardware-, Software- oder Anwendungsfehlern oder von Cyberangriffen. Die Sicherung von Daten/Programmen und deren Wiederherstellung nach Daten/Programmverlusten ist damit wesentlich für die Sicherstellung der Systemverfügbarkeit. Bei Systemen, die von externen IT-Dienstleistern betrieben werden (Outsourcing, Cloudlösungen), dient eine zusätzliche lokale Datensicherung außerdem zur Vorsorge von Problemen, Ausfällen oder der Insolvenz des externen IT-Dienstleisters.

Umsetzung:

Die Realisierung der Datensicherung muss mit einer geeigneten Sicherheitssoftware auf Sicherungsmedien (SAN/NAS, Bandlaufwerke mit Magnetbändern, ...) erfolgen. Die Sicherungsmedien müssen dabei räumlich von den zu sichernden IT-Systemen getrennt aufgestellt werden (Vorsorge gegen Feuer u. ä.). Zur Vorsorge von nicht sofort erkannten Datenverlusten/-manipulationen sind mehrere Sicherungsgenerationen vorzusehen (Tages-, Wochen-, Monatssicherungen). Bei besonders kritischen Systemen muss eine Wiederherstellung bis zur letzten Speicherung/Transaktion realisiert werden.

Erfolgt die Datensicherung auf stationären Speichermedien (SAN, NAS), so ist eine automationsgestützte (physische) Trennung des Speichermediums nach dem Abschluss der Datensicherung erforderlich (AirGap). Diese Maßnahme dient der Vorsorge für eine Verschlüsselung des Sicherungsmediums bei Cyberangriffen mittels eines Kryptotrojaners.

Das Vorgehen für die Wiederherstellung von Datensicherungen muss dokumentiert und regelmäßig geprüft werden.

Bei IT-Systemen, die von externen IT-Dienstleistern betrieben werden (Outsourcing, Cloudlösungen) ist (neben der Sicherung des externen IT-Dienstleisters) auch eine zusätzliche lokale Sicherung auf eigenen Sicherungsmedien vorzusehen, um im Fall von Problemen/Ausfall/Insolvenz des externen IT-Dienstleisters zumindest auf die eigenen Daten weiter zugreifen zu können.

Sicherstellung der Herstellerunterstützung [STARK EMPFOHLEN]

> **Ziele/Nutzen**: Durch die Herstellerunterstützung (Wartung) von IT-Systemen wird u.a. die Behebung von Fehlern, Problemen und Sicherheitslücken sowie die Versorgung mit Ersatzteilen (bei Hardwarekomponenten) gewährleistet. Üblicherweise umfasst die Herstellerunterstützung (Wartung) auch die Anpassung von IT-Systemen an geänderte Rahmenbedingungen (z. B. geänderte gesetzliche Regelungen) sowie die Weiterentwicklung der IT-Systeme. Eine aufrechte Herstellerunterstützung ist daher wesentlich für die Sicherstellung der Systemverfügbarkeit und der IT-Sicherheit.

Umsetzung:

Es muss zumindest für alle wesentlichen IT-Systeme eine Wartungsvereinbarung, die zumindest die Behebung von Fehlern, Problemen und Sicherheitslücken (u. a. im Rahmen von Software-Patches und Updates) sowie die Versorgung mit Ersatzteilen (bei Hardwarekomponenten) umfasst, mit dem Hersteller/Lieferanten abgeschlossen werden. Darüber hinaus ist regelmäßig zu prüfen, ob die Herstellerunterstützung von eingesetzten IT-Systemen oder von einzelnen Systemversionen in Zukunft eingestellt werden soll (End of Life). Sollte dies der Fall sein, so sind rechtzeitig Maßnahmen zur Ablöse der betroffenen IT-Systeme oder für Systemupdates vorzusehen.

Laufendes Einspielen von kritischen Software-Patches / Updates [STARK EMPFOHLEN]

> **Ziele/Nutzen**: Das Einspielen von kritischen Software-Patches oder Updates dient zur Behebung von kritischen Fehlern oder Sicherheitslücken und ist damit sowohl das Funktionieren als auch für die Sicherstellung der Verfügbarkeit von IT-Systemen wesentlich.

Umsetzung:

Das Einspielen von Software-Patches oder Updates, die kritische Fehler oder Sicherheitslücken beheben, ist unverzüglich/zeitnah nach deren Veröffentlichung sicherzustellen. Dazu ist es auch erforderlich, sicherzustellen, dass eine Benachrichtigung des Herstellers über kritische Software-Patches oder Updates erfolgt (Notification der Hersteller, ...).

Test neuer Software / Software-Versionen [STARK EMPFOHLEN]

> **Ziele/Nutzen**: Durch die Überprüfung neuer Softwarekomponenten oder neuer Software-Versionen vor deren produktiver Nutzung werden die Funktionalitäten der Software, die korrekte Verarbeitung der Daten und das fehlerfreie Zusammenwirken mit verbundenen IT-Systemen geprüft. Diese Maßnahme ist wesentlich, um das anforderungsgerechte Funktionieren von IT-Systemen und deren

> Verfügbarkeit nach der Produktivsetzung zu gewährleisten.

Umsetzung:

Zumindest für wesentliche IT-Systeme sind vor deren produktiver Nutzung entsprechende Funktionalitäts- und Integrationstests auf Basis von vorher erstellten Testplänen vorzusehen. Zur Durchführung der Tests sind sowohl eine eigene Testinfrastruktur als auch die entsprechenden Personalressourcen notwendig.

Bei kritischen Software-Patches oder Updates kann aufgrund der zeitlichen Kritikalität die Testung entfallen.

Migrationsplanung für Versionsumstellungen und Vorsorge durch Rollback-Szenarien [STARK EMPFOHLEN]

> **Ziele/Nutzen**: Ziel der Migrationsplanung ist die Sicherstellung einer erfolgreichen Versionsumstellung (Patch, Update) von IT-Systemen auf Basis einer getesteten Software-Version und die Minimierung der Auswirkungen der Downtime des IT-Systems auf den Geschäftsbetrieb.

Umsetzung:

Im Rahmen der Migrationsplanung ist der Ablauf der Versionsumstellung (Patch, Update) mit den entsprechenden Zuständigkeiten festzulegen und der Zeitpunkt der Migration so zu wählen, dass die Auswirkungen auf den Geschäftsbetrieb so gering wie möglich sind. Vor der Inbetriebnahme einer neuen Version des IT-Systems ist u.a. die erfolgreiche Datenübernahme aus der Vorversion zu prüfen.

Als Vorsorge für eine fehlerhafte Datenübernahme oder sonstige Mängel, die erst nach der Versionsumstellung erkennbar sind, ist zumindest für wesentliche IT-Systeme ein Rollback-Szenario vorzusehen, mit dem wieder auf die Vorversion zurückgewechselt werden kann. Bei kritischen Software-Patches oder Updates kann aufgrund der zeitlichen Kritikalität das Rollback-Szenario entfallen.

Vereinbarung von Servicelevels (bei Systemoutsourcing / Cloudservices) [STARK EMPFOHLEN]

> **Ziele/Nutzen**: Bei IT-Systemen, die von externen IT-Dienstleistern betrieben werden (Outsourcing, Cloudlösungen) besteht kein direkter Einfluss auf den internen Systembetrieb. Zur Sicherstellung der erforderlichen Verfügbarkeit und Nutzbarkeit ist daher eine entsprechende vertragliche Absicherung der einzuhaltenden Servicelevels erforderlich.

Umsetzung:

Die Vereinbarung der erforderlichen Servicelevels ist in den vertraglichen Vereinbarungen mit dem externen IT-Dienstleister entsprechend zu berücksichtigen. Die Vereinbarung von Servicelevels erfolgt im Rahmen

eines Service-Level-Agreements (SLA) und sollte dabei u. a. garantierte Mindestwerte für die grundsätzliche Verfügbarkeit des IT-Systems, die Systemperformance, die Reaktionszeiten bei Fehlern / Problemen / Sicherheitsverletzungen sowie für die max. Systemwiederherstellungsdauer nach Ausfällen beinhalten. Bei dem SLA ist auch die Erbringung des Nachweises der Einhaltung der vereinbarten Servicelevels durch den externen IT-Dienstleister festzulegen. Bei der Überschreitung von Servicelevels sind entsprechende Korrekturmaßnahmen und/oder Pönalzahlungen vorzusehen.

Bei besonders kritischen IT-Systemen kann auch eine regelmäßige Auditierung der Maßnahmen zur Erreichung der Servicelevels beim externen IT-Dienstleister vorgesehen werden.

Die Vereinbarung eines SLA kann auch mit einer internen IT-Abteilung oder einem internen IT-Dienstleister zur Sicherstellung der notwendigen Servicequalität sinnvoll sein.

DDoS-Schutz [STARK EMPFOHLEN]

> **Ziele/Nutzen**: Der Schutz vor Distributed Denial of Service-Attacken (DDoS) dient der Abwehr von Überlastungsangriffen, deren Ziel es ist, die Verfügbarkeit von IT-Systemen zu beeinträchtigen oder zu unterbrechen.

Umsetzung:

Zumindest für wesentliche IT-Systeme, die aus dem Internet erreichbar sind, sind entsprechende Schutzdienste gegen DDoS-Attacken einzurichten (Load Balancer, DDoS-Schutzdienste, ...). Das kann in der eigenen IT-Infrastruktur erfolgen oder durch vorgelagerte Sicherheitsdienstleister.

Dokumentation aller (wesentlichen) IT-Systeme [STARK EMPFOHLEN]

> **Ziele/Nutzen**: Sowohl zur Planung und Umsetzung von Maßnahmen zur Informationssicherheit als auch zur Bewältigung von Fehlern und Problemen (inkl. Cybergefahren und Cyberangriffe) sind relevante Informationen über die genutzten IT-Systeme und deren Zusammenwirken notwendig.

Umsetzung:

Zumindest wesentliche IT-Systeme (Hardware und Software!) sind ausreichend zu dokumentieren. Dazu zählen neben allgemeinen Angaben (Bezeichnung, Hersteller, Version, ...) auch Informationen über Abhängigkeiten zu anderen IT-Systemen und wesentliche Prozesse zur Systemadministration

Erstellung von Notfallplänen für den Ausfall von IT-Systemen [STARK EMPFOHLEN]

>

> **Ziele/Nutzen**: Für wesentliche IT-Systeme sind als Vorsorge für einen Totalausfall entsprechende Notfallpläne notwendig. Ziel dieser Notfallpläne ist eine möglichst rasche Wiederherstellung der betroffenen IT-Systeme sowie Maßnahmen zur Aufrechterhaltung des Geschäftsbetriebs während des Ausfalls.

Umsetzung:

Für alle wesentlichen IT-Systeme sind Notfallpläne zu erstellen, die

- die Wiederherstellung und den Wiederanlauf des betroffenen IT-Systems unter Berücksichtigung aller technischen Abhängigkeiten beschreiben,
- etwaige notwendige, organisatorische Maßnahmen zur Aufrechterhaltung des Geschäftsbetriebs während des Ausfalls beschreiben,
- die notwendige Kommunikation im Rahmen der Notfallbewältigung definieren und
- die Zuständigkeiten und Entscheidungsstrukturen im Rahmen der Notfallbewältigung festlegen.

Ist im Rahmen eines Notfalls die Wiederherstellung mehrerer IT-Systeme erforderlich, so ist eine Reihenfolge der Wiederherstellung auf Basis der Kritikalität der IT-Systeme für die Organisation sowie auf Basis der Abhängigkeiten zwischen den IT-Systemen festzulegen.

er
C
C
0
b
er
ei
tg
e
st
ell