A08 Checkliste IT-System

Computersysteme in ortsfesten Befehlsstellen (Windows 10 Professional)

Tipp: Genauere Informationen zur Umsetzung dieser Checkliste finden Sie im **Anhang 09** Administrationshandbuch, welches im Intranet des Befehlsstellensystems für technische Ansprechpartner abrufbar sind.

P/E	Anforderung	**Umgesetzt? (Ja/Nein)**
P	**Sichere Installation und Konfiguration** Um mögliche Ursachen für Computerfehler zu reduzieren und ungewollte Datenübertragungen an Microsoft und anderen Drittanbieter auszuschließen, sollten nur für die Aufgabenwahrnehmung notwendige Komponenten und Programme auf dem Windows 10-Computersystem installiert werden. Die Installation und Konfiguration der IT-Systeme sollte vor Ort von Personen mit Computerkenntnissen durchgeführt werden [SYS2.1.A15; SYS2.1.A16, SYS2.2.3.A4; SYS2.2.3.A13; SYS2.2.3.A14; SYS2.2.3.A15; SYS2.2.3.A16].	
P	**Keine Netzkopplung** Die Kopplung zwischen dem Befehlsstellennetz und anderen Netzwerken, z.B. dem Internet und anderen Netzen ist nicht zulässig. Unter einer Netzkopplung wird auch das zeitweilige Einbinden des Computersystems der Befehlsstelle in ein anderes Netzwerk verstanden. Eine Nicht-Beachtung stellt eine zusätzliche Gefährdung für die Verfügbarkeit, Integrität und Vertraulichkeit des gesamten Befehlsstellennetzes sowie der IRLS Lausitz dar, da z.B. somit die Möglichkeit besteht, Schadcode in das geschlossene Netzwerk zu übertragen [SYS3.1.A8]. **Eine Nichtbeachtung führt zur Sperrung des Netzzugangs.**	
P	**Aktualisierung des Betriebssystems** Das Betriebssystem ist regelmäßig mit Sicherheitspatches und Updates zu aktualisieren. Der Client ist so einzurichten, dass automatisch Patches & Updates heruntergeladen und installiert werden [SYS2.1.A3; SYS2.1.A14]. **Hinweis:** Um die Sicherheitspatches und Updates für das Betriebssystem im geschlossenen Netzwerk zu erhalten, stellt die IRLS Lausitz einen Update-Dienst zentral bereit.	
P	**Rollentrennung** Das Computersystem ist so einzurichten, dass die typische Nutzung als Befehlsstelle nicht mit Administrationsrechten erfolgt. Nur Administratoren dürfen Administrationsrechte erhalten, um die Systemkonfiguration zu ändern, Anwendungen zu installieren und zu entfernen [SYS2.1.A13].	
P	**Anbindung an zentralen Zeitgeber (NTP-Server)** Der Befehlsstellenclient ist an den zentralen Zeitserver der IRLS Lausitz anzubinden. Damit wird die Datenintegrität sichergestellt und Widersprüche vermieden, indem die identische Zeit in der Befehlsstelle bereitsteht. **Hinweis:** Die Uhrzeit wird automatisch über das Netzwerk verteilt.	
P	**Einsatz eines Virenschutzprogramm** Auf dem Befehlsstellencomputer ist ein Virenschutzprogramm einzusetzen. Die IRLS Lausitz stellt zentral ein Virenschutzprogramm zur Verfügung und liefert regelmäßig Updates [SYS2.1.A6; SYS2.2.3.A5].	
P	**Fernwartung** Im Störungsfall ist eine schnelle Unterstützung von großem Vorteil. Zu diesem Zweck ist die Einrichtung einer Fernwartungsanwendung erforderlich, diese ist am Befehlsstellenclient durch den Administrator vor Ort zu installieren und zu konfigurieren.	

E	**Systemüberwachung** Der Befehlsstellenclient ist in das Monitoring-System der IRLS Lausitz einzubinden. Darüber werden der Systemzustand und die Funktionsfähigkeit des Clients laufend überwacht und Fehlerzustände sowie die Überschreitung definierter Grenzwerte an das administrative Personal vor Ort gemeldet. In der Folge werden Störungsquellen, Gefährdungen rechtzeitig erkannt und behoben. Dadurch erhöht sich die Betriebssicherheit des Befehlsstellenclients [SYS2.1.A29; SYS2.1.A41].	
E	**Benutzerauthentisierung** Der Zugang zu den durch die IRLS Lausitz bereitgestellten Anwendungen wird durch separate Zugangsdaten geschützt. Die Benutzerauthentisierung am Betriebssystem (z.B. durch Abfrage von Benutzername und Passwort) ist dennoch empfehlenswert, insbesondere da vertrauliche Informationen auf dem Computersystem gespeichert werden [SYS2.1.A1; SYS2.2.3.A17].	
E	**Regelmäßige Datensicherung** Es gibt unterschiedliche Gründe für Datenverluste, häufig sind defekte Festplatten oder Computerviren ein Grund. Sofern ein Datenverlust eingetreten ist, ist die Rettung eine Datensicherung. Empfehlenswert ist daher die regelmäßige Datensicherung des Computersystems, um schnell wieder betriebsfähig zu sein. Dabei sollte die Sicherungskopie nicht aktiv mit dem Computersystem verbunden sein (Offline-Sicherung). Ferner sollten Sie regelmäßig testen, ob eine Datenwiederherstellung möglich ist. **Hinweis:** Die Sicherungskopien enthalten eine vollständige Kopie des Computersystems und sollten dementsprechend sicher verwahrt und vor unberechtigten Zugriff geschützt werden.	
E	**Bildschirmsperre** Nicht immer ist es erforderlich, dass ein aktiver Befehlsstellencomputer genutzt wird. Dadurch besteht für unberechtigte Personen die Möglichkeit, Zugriff auf die vertraulichen Einsatzdaten zu gelangen. Empfehlenswert ist die Einrichtung einer Bildschirmsperre, die nach einer gewissen Zeit automatisiert den Computerzugriff sperrt und zur Reaktivierung eine Benutzerauthentifizierung verlangt.	
E	**Absicherung des Boot-Vorgangs** Der Startvorgang des Computersystems, dass sogenannte "Booten" muss gegen Manipulationen abgesichert werden. Dafür muss vom Administrator vor Ort festgelegt werden, von welchen Medien gebootet werden darf. Es ist sicherzustellen, dass nur Administratoren die Clients von einem anderen als den voreingestellten Laufwerken oder externen Speichermedien booten können [SYS2.1.A8; SYS2.1.A36].	
E	**Datei- und Freigabeberechtigungen** Der Zugriff auf Dateien und Ordner auf dem lokalen System sowie auf Netzwerkfreigaben ist so gering wie möglich zu halten. Sie sollten die Speicherung von vertraulichen Daten in Freigabeordnern vermeiden [SYS.2.2.3.A12].	
E	**Umgang mit Wechseldatenträgern** Über Wechseldatenträger, z.B. USB-Sticks, Speicherkarten, CDs, DVDs usw. kann Schadcode auf das Computersystem gelangen und es können vertrauliche Daten kopiert und unberechtigt entwendet werden. Um diese Gefährdungen auszuschließen, ist die Einschränkung der Nutzung von Wechseldatenträgern empfehlenswert [SYS2.1.A24]	
E	**Verschlüsselung des Computersystems** Wenn vertrauliche Informationen auf dem Computersystem gespeichert werden, z.B. Einsatzberichte als PDF-Datei o.ä., sollten die schutzbedürftigen Dateien, ausgewählte Dateisystembereiche oder besser die gesamte Festplatte verschlüsselt werden [SYS2.1.A28, SYS2.2.3.A21].	

E	**Personal-Firewall** Auf dem Betriebssystem des Befehlsstellenclients sollte die Personal Firewall aktiv sein. Die Filterregeln der Firewall sollten so restriktiv wie möglich sein. Sie sind regelmäßig zu testen. Die Personal Firewall ist so zu konfigurieren, dass die Benutzer nicht durch Warnmeldungen belästigt werden, die sie nicht interpretieren können [SYS 2.1.A31].	
E	**Windows PowerShell** Die Ausführung der PowerShell sowie von WPS-Dateien sollte nur für Administratoren vor Ort erlaubt sein [SYS2.2.3.A22].	
E	**Unterbrechungsfreie Stromversorgung** Der Befehlsstellenclient sollte an eine unterbrechungsfreie Stromversorgung (USV) angeschlossen werden. Die USV sollte hinsichtlich Leistung und Stützzeit ausreichend dimensioniert sein. Sowohl für die USV-Geräte als auch die Clients sollte ein Überspannungsschutz vorhanden sein [SYS2.1.A39]. **Hinweis:** Die tatsächliche Kapazität der Batterie und damit die Stützzeit der USV sollte regelmäßig getestet werden. Die USV sollte regelmäßig gewartet werden. **Tipp:** Notebooks enthalten einen Akku, der eine plötzliche Unterbrechung der Stromversorgung ohne großen Aufwand kompensieren kann. Ein Überspannungsschutz ist bei dieser Variante aber weiterhin erforderlich.	
E	**Regelmäßige Betriebsdokumentation** Die Durchführung von betrieblichen Aufgaben an Clients sollte nachvollziehbar dokumentiert werden (Wer? Wann? Was?). Aus der Dokumentation heraus sollten insbesondere Konfigurationsänderungen nachvollziehbar sein. Auch Aufgaben (wer ist z. B. befugt, Änderungen durchzuführen) sollten festgelegt und dokumentiert werden. Die Dokumentation sollte gegen unbefugten Zugriff und Verlust geschützt werden [SYS2.1.A40].	

Computersysteme in mobilen Befehlsstellen (z.B. Tablets /Laptop / Notebooksystem (Windows 10 Professional)

Aufgrund der leichteren Mobilität eines Laptops / Notebooks werden zusätzliche Anforderungen als verpflichtend deklariert, welche im Bereich „Computersysteme“ nur als Empfehlung genannt wurden. Die zusätzlich verpflichtenden Maßnahmen sind bei Notebooks / Laptops umzusetzen und werden deshalb nochmals erwähnt.

P/E	Anforderung	Umgesetzt? (Ja/Nein)
P	**Benutzerauthentisierung** Der Zugriffschutz auf das Betriebssystem (z.B. durch Abfrage von Benutzername und Passwort, Smartcard o.ä.) ist umzusetzen, um den Zugang zu sensiblen Anwendungen und den Zugriff auf vertrauliche Daten in unsicheren Arbeitsumgebungen für Unberechtigte zu erschweren [SYS2.1.A1; SYS2.2.3.A17].	
P	**Bildschirmsperre** Es ist eine Bildschirmsperre mit Zugriffsschutz einzurichten, die nach einer gewissen Zeit automatisiert den Computerzugriff sperrt und zur Reaktivierung eine Benutzerauthentifizierung verlangt. Die Benutzer sind angehalten, beim Verlassen des mobilen Arbeitsplatzes den Computer zu sperren.	
P	**Absicherung des Boot-Vorgangs** Der Startvorgang des Computersystems, dass sogenannte "Booten" muss gegen Manipulationen abgesichert werden. Dafür muss vom Administrator vor Ort festgelegt werden, von welchen Medien gebootet werden darf. Es ist sicherzustellen, dass nur Administratoren die	

	Clients von einem anderen als den voreingestellten Laufwerken oder externen Speichermedien booten können [SYS2.1.A8; SYS2.1.A36].	
P	**Verschlüsselung des Laptops / Notebooks** Da vertrauliche Informationen auf dem Computersystem gespeichert werden, z.B. Einsatzberichte als PDF-Datei o.ä., sollten die schutzbedürftigen Dateien, ausgewählte Dateisystembereiche oder besser die gesamte Festplatte verschlüsselt werden [SYS2.1.A28, SYS2.2.3.A21; SYS3.1.A13].	
P	**Personal-Firewall** Auf dem mobilen Befehlsstellenclient ist die Personal Firewall zu aktivieren. Die Filterregeln der Firewall sollten so restriktiv wie möglich sein. Sie sind regelmäßig zu testen. Die Personal Firewall ist so zu konfigurieren, dass die Benutzer nicht durch Warnmeldungen belästigt werden, die sie nicht interpretieren können [SYS 2.1.A31; SYS3.1.A3].	
E	**Geeignet Auswahl von Laptops / Notebooks** Bevor Laptops für mobile Befehlsstellen beschafft werden, SOLLTE die Anforderungen ermittelt werden, z.B. Robustheit, Akkulaufzeit, Lesbarkeit des Displays bei Tageslicht usw. Anhand der Ergebnisse SOLLTEN alle infrage kommenden Geräte bewertet werden [SYS.3.1.A15].	
E	**Geeignete Aufbewahrung und Diebstahlschutz von Laptops / Notebooks** Es sollten klare Regeln festgelegt werden, wie das Laptop / Notebook bei Nichtnutzung außerhalb der Befehlsstelle aufzubewahren sind. Auch innerhalb der Befehlsstelle sollte außerhalb der Nutzungszeiten das Gerät gut gegen Diebstahl gesichert und folgerichtig verschlossen aufbewahrt werden [SYS3.1.A14; SYS3.1.A18].	

Netzwerktechnik / Router

P/E	Anforderung	**Umgesetzt? (Ja/Nein)**
P	**Geeignete Aufstellung** Das Endgerät ist so aufzustellen, dass möglichst nur befugte Personen einen Zutritt erhalten.	
E	**Unterbrechungsfreie Stromversorgung** Das Endgerät sollte an eine unterbrechungsfreie Stromversorgung (USV) angeschlossen werden. Die USV sollte hinsichtlich Leistung und Stützzeit ausreichend dimensioniert sein. Sowohl für die USV-Geräte als auch für die gesamte Netzwerktechnik sollte ein Überspannungsschutz vorhanden sein. **Hinweis:** Die tatsächliche Kapazität der Batterie und damit die Stützzeit der USV sollte regelmäßig getestet werden. Die USV sollte regelmäßig gewartet werden.	

Drucker / Multi-Funktions-Center / Faxgerät

P/E	Anforderung	**Umgesetzt? (Ja/Nein)**
P	**Anbindung an zentralen Zeitgeber (NTP-Server)** Netzwerkfähige Drucker und Multifunktionsgeräte im Befehlsstellennetz sind an den zentralen Zeitserver der IRLS Lausitz anzubinden. Damit wird die Datenintegrität sichergestellt und Widersprüche vermieden, indem die identische Zeit auf Ausdrucken bereitgestellt wird. **Hinweis:** Genauere Informationen zur Realisierung finden Sie in der Bedienungsanleitung ihre Netzwerkdruckers.	
P	**Regelmäßige Aktualisierung** Es ist regelmäßig zu prüfen, ob der Drucker bzw. das Multifunktionscenter auf dem aktuellen Stand ist. Beim Einspielen von Patches und Updates ist darauf zu achten, dass die Aktualisierungen von vertrauenswürdigen Quellen stammen.	
P	**Beschränkung der Administrationszugriffe** Der Zugriff auf die Konfiguration des Endgerätes ist zu beschränken. Dazu ist das Standardpasswort bei Auslieferung zu ändern [SYS4.1.A7].	
P	**Verschlüsselte Verbindung** Um Alarmausdrucke von der Leitstelle zu erhalten, ist die Anbindung an den Druckserver der IRLS Lausitz über das Internet-Printing-Protocol-Secure (IPPS) zulässig [SYS4.1.A7].	
E	**Geeignete Aufstellung** Das Endgerät ist so aufzustellen, dass möglichst nur befugte Personen einen Zugriff auf Ausdrucke haben. Der Drucker sollte nicht in Bereichen aufgestellt werden, in denen sich häufig externe Personen, z.B. Gäste aufhalten. Also zum Beispiel nicht oder in der Nähe von Besprechungs- oder Schulungsräumen [SYS4.1.A2].	
E	**Versorgung und Kontrolle der Verbrauchsgüter** Drucker, Kopierer und Multifunktionsgeräte sind auf Verbrauchsgüter wie Papier oder Toner angewiesen, um funktionieren zu können. Die Versorgung mit diesen Verbrauchsgütern sollte in der Befehlsstelle sichergestellt sein. Die Entsorgung der Verbrauchsgüter sollte geregelt werden.	
E	**Unterbrechungsfreie Stromversorgung** Das Endgerät sollte an eine unterbrechungsfreie Stromversorgung (USV) angeschlossen werden. Die USV sollte hinsichtlich Leistung und Stützzeit ausreichend dimensioniert sein. Sowohl für die USV-Geräte als auch für den Drucker bzw. das Multifunktionsgerät sollte ein Überspannungsschutz vorhanden sein. **Hinweis:** Die tatsächliche Kapazität der Batterie und damit die Stützzeit der USV sollte regelmäßig getestet werden. Die USV sollte regelmäßig gewartet werden.	
E	**Ordnungsgemäße Entsorgung** Zur Entsorgung von nicht mehr benötigten vertraulichen Ausdrucken, z.B. Einsatzberichte, sollten geeignete Entsorgungseinrichtungen vorhanden und betriebsfähig sein, z.B. Aktenvernichter. Wird das vertrauliche Material zunächst gesammelt und später entsorgt, sollte dieser von unberechtigtem Zugriff geschützt werden.	