Weisung W111: Anforderungen nichtkantonale Geräte und deren Verwendung

Version 1.0; 22. Februar 2017

Diese Regelung stützt sich auf § 21 Absatz 4a der Verordnung über die Informatiksicherheit und über die Nutzung von Informatikmitteln (Informatiksicherheitsverordnung, SRL Nr. 26b) vom 22. November 2016.

I. Einleitung

Zweck: Festlegung der minimalen Konfigurationsstandards für nichtkantonale Geräte, welche für die Bearbeitung von Informationen des Kantons Luzern benutzt werden und Festlegung des korrekten Umgangs mit solchen Geräten.

Geltungsbereich:

- Geltungsbereich richtet sich nach § 2 der Informatiksicherheitsverordnung
- Vertragspartner mit Zugriff auf kantonale Informatikmittel und Informationen des Kantons Luzern

Adressaten: Mitarbeitende und Lernende im Geltungsbereich

Quellen: keine

II. Abgrenzung

Ausgenommen sind in öffentlichen Netzwerken (Internet) verfügbare Informatikservices, welche der Informationsbeschaffung der Bürger dienen. Dazu gehören beispielsweise der Internetauftritt des Kantons Luzern oder die Internetauftritte der Departemente.

III. Anforderungen an nichtkantonaler Geräte

Nichtkantonale Geräte, die zur Bearbeitung von Informationen des Kantons Luzern benutzt werden sollen, müssen die folgenden Mindestanforderungen erfüllen. Die Organe können weitere Anforderungen vorgeben.

III.1 Mobiltelefone, Tablets

- Es dürfen nur Betriebssysteme und Software auf den Geräten installiert sein, welche vom Hersteller mit Sicherheitsupdates versorgt werden.
- Es sind immer die aktuellsten Sicherheits-Updates des jeweiligen Betriebssystems und der installierten Software auf die Geräte zu laden und anzuwenden.
- Es darf nur rechtmässig lizenzierte Software installiert und verwendet werden.
- Das Betriebssystem ist im vom Hersteller unterstützten Modus zu betreiben. Es darf kein sogenannter Jailbreak[1] (iOS) oder ein Rooten[2] (Android) durchgeführt worden sein.
- Falls möglich: aktives Antivirus-Programm mit den jeweils aktuellsten Virendefinitionen.
- Es darf keine Software installiert sein, welche für Angriffe auf die Infrastruktur des Kantons Luzern verwendet werden kann (§ 21 Abs. 4d Informatiksicherheitsverordnung).
- Die unterstützten Betriebssysteme sowie die verwendeten bzw. unterstützten Apps und Programme werden von den zuständigen Departementen vorgegeben.
- Die Verwendung der Geräte darf den Dienstbetrieb nicht erschweren oder einschränken (§ 21 Abs. 4e Informatiksicherheitsverordnung).

III.2 Computer, weitere Geräte

- Es dürfen nur Betriebssysteme und Software auf den Geräten installiert sein, welche vom Hersteller mit Sicherheitsupdates versorgt werden.

[1] https://de.wikipedia.org/wiki/Jailbreak_(iOS)
[2] https://de.wikipedia.org/wiki/Rooten

- Es sind immer die aktuellsten Sicherheits-Updates des jeweiligen Betriebssystems und der installierten Software auf die Geräte zu laden und anzuwenden.
- Es darf nur rechtmässig lizenzierte Software installiert und verwendet werden.
- Es muss ein aktives Antivirus-Programm mit den aktuellsten Virendefinitionen installiert und in Betrieb sein; falls unterstützt, muss die heuristische Erkennung aktiviert sein.
- Die verwendeten beziehungsweise unterstützten Programme werden von den zuständigen Departementen vorgegeben.
- Es darf keine Software installiert sein, welche für Angriffe auf die Infrastruktur des Kantons Luzern verwendet werden kann (§ 21 Abs. 4d Informatiksicherheitsverordnung).
- Wird für den Zugriff auf Informationen oder Systeme des Kantons Luzern eine VPN-Verbindung verwendet, ist kein Split-Tunnel[3] erlaubt.
- Die Verwendung der Geräte darf den Dienstbetrieb nicht erschweren oder einschränken (§ 21 Abs. 4e Informatiksicherheitsverordnung).
- Minimal unterstützte Betriebssysteme (z.B. für Programme):
    - Windows 7 32bit
    - Windows 7 64bit
    - Windows 10 64bit
- Minimal unterstützte Browser (z.B. für Webanwendungen):
    - Microsoft Internet Explorer 11

IV. Umgang mit den Geräten und Informationen

- Während des Zugriffs auf Informationen, Services oder Systeme des Kantons Luzern darf nur der für die Benutzung des Geräts autorisierte Benutzer dieses benutzen.
- Nichtkantonale Informationen sind getrennt von Informationen des Kantons Luzern zu speichern.
- Werden als vertraulich oder geheim klassifizierte Informationen des Kantons Luzern auf dem nichtkantonalen Gerät gespeichert, sind diese zu verschlüsseln. Werden solche Informationen auf weitere Geräte ausgelagert, gilt die Vorschrift auch für diese Geräte.
  Vorgaben zu den zu verwendenden Algorithmen finden sich in Weisung der W105: Crypto Policy.
- Informationen des Kantons Luzern sind frühestmöglich sicher zu löschen, spätestens nach der vertraglich festgelegten Dauer, nach dem Projektende oder nach dem Vertragsende. Wird das Gerät ersetzt, abgelöst, weitergegeben oder soll es repariert werden, sind die Informationen des Kantons Luzern vorgängig sicher zu löschen.
  Vorschriften zur Löschung finden sich in der Weisung W104: Sicheres Löschen kantonaler Daten.

Der Kanton Luzern behält sich vor, Informationen und Software auf nichtkantonalen Geräten aus Sicherheitsgründen zu löschen (§ 21 Abs. 4c Informatiksicherheitsverordnung).

V. Benutzermanagement

Für die verwendeten Benutzerkonto für den Zugang zur Infrastruktur des Kantons Luzern gelten die Vorgaben der Weisung W101: Benutzername und Passwörter (Passwort-Policy).
Weiter gilt:

- Der Zugang zum Gerät ist mit einem Passwort zu schützen.
- Die Weitergabe der persönlichen kantonalen Zugangsdaten ist nicht gestattet.
- Zugangsdaten sind gemäss Prozess zu beantragen und zu übergeben (§ 13 Abs. 3 Informatiksicherheitsverordnung).

[3] https://de.wikipedia.org/wiki/Split_Tunneling

Dokumentenlenkung

Version	1.0	**Datum Erstellung**	22.02.2017
Dokumentbesitzer	DIIN CISO/MUM	**Datum Freigabe**	16.03.2017
Tritt in Kraft per:	01.04.2017		
Freigegeben durch	Informationssicherheitsbeauftragter, OVG		
Übergeordnete Dokumente	- Informatikgesetz vom 7. März 2005 (SRL Nr. 26) - Informatiksicherheitsverordnung vom 11. November 2016 (SRL Nr. 26b) - Network Security Policy vom 31. Januar 2017		
Mitgeltende Dokumente	- W101: Benutzernamen und Passwörter (Passwort-Policy) - W104: Sicheres Löschen kantonaler Daten		
Weiterführende Dokumente	keine		