Regelung zur externen Erreichbarkeit von vernetzten Endgeräten an der WWU

Diese Regelung gilt für alle im Datennetz der WWU betriebenen Endgeräte.

1) **Firewall mit „Whitelisting“ am Uni-Internet-Übergang**

Grundsätzlich sind keine Verbindungen von extern (z.B. aus dem Internet) auf interne Datenendgeräte der WWU möglich, es sei denn sie sind in einer „Whitelist“ für von extern erreichbare Dienste erfasst. Diese Einschränkung hat keine Auswirkung auf die interne Nutzung von intern angebotenen Diensten. Auch die Nutzung von externen Diensten/Servern durch interne Endgeräte ist hierdurch nicht eingeschränkt. Durch die Nutzung von VPN können interne Endgeräte über das Internet erreicht werden.

2) **Erfassung und Verwaltung von Endgeräten mit Diensten, die von extern erreichbar sein müssen**

Zu jedem Endgerät wird angegeben, ob und welche (externen) Dienste angeboten werden. Diese Informationen lassen sich neben der Firewall-Konfiguration für Statistiken in den IVVen, zur Information bei Sicherheitslücken und für den Security Audit verwenden.

3) Verwendung öffentlicher IP-Adressen nur noch in begründeten Fällen

Endgeräte bekommen zukünftig grundsätzlich private IP-Adressen zugeteilt. Damit ist die Erreichbarkeit aus dem Internet generell unterbunden. Für die Nutzung von externen Diensten/Servern kann im Bedarfsfall eine NAT-Funktionalität eingerichtet werden. Öffentliche IP-Adressen werden nur noch in begründeten Ausnahmefällen zugeteilt. Bereits zugewiesene öffentliche IP-Adressen können beibehalten werden.

4) Proaktive Portscans

Bei akuten Bedrohungen, können vom ZIV Sicherheitsscans auf einzelne verwundbare Dienste/Ports gemacht werden, um Sicherheitslücken zu erkennen. Alle Endgeräte, die aus dem Internet erreichbar sind, werden regelmäßig vom ZIV auf Sicherheitslücken gescannt. Der DFN-Verein empfiehlt, das eigene Netz zur Vorbeugung zu scannen.

Anhang

Umsetzung

1) Im ersten Schritt werden vom ZIV und den IVVen die Subnetze abgefragt, welche aus dem Internet erreichbar sein sollen und welche nicht.
2) Die Subnetze, die nicht erreichbar sein sollen, und Subnetze, zu denen keine Information bzgl. notwendiger Erreichbarkeit vorliegt, werden ab einem Stichtag nicht mehr aus dem Internet erreichbar sein.
3) Für noch erreichbare Subnetze müssen bis zu einem Stichtag alle Endgeräte und Dienste, die weiterhin aus dem Internet erreichbar sein sollen, im ZIV angemeldet werden (Verwaltung einer „Whitelist“). Die Anmeldung erfolgt über den IV-Sicherheitsbeauftragten (bzw. den IVV-Leiter). Das ZIV behält sich vor, die Anmeldungen auf Plausibilität zu prüfen.
4) In einem jährlichen Reporting bekommt jede IVV eine Übersicht der erreichbaren Endgeräte und ihrer Dienste. Für jedes der Endgeräte ist jährlich ein „Verlängerungsantrag“ erforderlich. Endgeräte, die über einen längeren Zeitraum nicht aktiv sind, werden aus der Whitelist entfernt.
5) In Zukunft werden für Endgeräte grundsätzlich private IP-Adressen vergeben (mit optionaler NAT-Funktionalität). Nur in begründeten Ausnahmefällen werden öffentliche IP-Adressen vergeben.

Netzbereiche

1) **Angemeldete Endgeräte**: Zum **internen** Netz der WWU (Intranet) zählen alle im ZIV angemeldeten Endgeräte. Aktuell ist dabei keine Unterscheidung zwischen Endgeräten der WWU und des UKMs möglich. Das Netz des **UKM** wird als **intern** betrachtet, damit den Wissenschaftlern weiterhin der Zugang zu Uni-Systemen erhalten bleibt.
2) **Nicht angemeldete Endgeräte**: Zum Einwahlbereich der WWU gehören größtenteils private, nicht von der WWU verwaltete Endgeräte, die per WLAN, pLANet.X oder VPN an das Netz der WWU angeschlossen werden.
    a. WLAN und pLANet.X bieten einen Internetzugang für Berechtigte an. Durch den eduroam-Dienst gehören zum Nutzerkreis auch WWU-Externe. Grundsätzlich ist die Sicherheit des WLAN gegenüber dem Intranet durch die dabei verwendeten Endgeräte als niedriger anzusehen. Der Einwahlbereich **WLAN** sollte deshalb grundsätzlich als **extern** angesehen werden.
    b. Bei der VPN-Einwahl handelt es sich (ebenso wie beim WLAN) um einen Netzzugang von nicht verwalteten Endgeräten. Die VPN-Zugänge wurden allerdings ganz bewusst dafür eingerichtet, eine Einwahl in das WWU-interne Netz und die Nutzung interner Dienste zu ermöglichen. Daher soll der Bereich der **VPN-Zugänge** als **intern** angesehen werden. Da die Einführung des Whitelisting insgesamt eine substanzielle Verbesserung im Bereich IT-Sicherheit bedeutet, werden die durch diese Zuordnung bestehenden Risiken zunächst in Kauf genommen. Die Alternativen (Design-Änderung des VPN-Service oder Alternativen zum VPN-Service) sollen untersucht werden.