Netze für IT-Systeme ohne Support

Systeme, die vom Hersteller nicht länger mit Sicherheits-Updates etc. versorgt werden, dürfen an der TU Braunschweig laut der "Richtlinie zum Umgang mit IT-Systemen ohne Support" nur noch im Rahmen eines Ausnahmeverfahrens und ggf. unter Auflagen (nach Genehmigung des IT-Security-Boards) betrieben werden. Eine Möglichkeit zum Weiterbetrieb besteht in der Ausgliederung dieser Systeme in ein privates, vom Rest der IT an der TU-Braunschweig gekapseltes lokales Netzwerk (... siehe Handreichung der Stabsstelle CISO zur oben genannten Richtlinie). Dies wird von der Abteilung Netze am Gauß-IT-Zentrum wie folgt unterstützt, wobei die vorliegende Handreichung lediglich ein (mit der Stabsstelle CISO abgestimmtes) Konzept beschreibt, das von den Einrichtungen jedoch in Eigenverantwortung umgesetzt werden muss.

Wie sieht ein solcher Aufbau aus?

Ganz einfach gesagt wird für die alten Systeme ein separates Netz gebaut. Dies kann, je nach lokalen Gegebenheiten wie folgt geschehen:

- Systeme stehen physisch nah beieinander: Die Systeme werden über einen separaten, lokalen Switch vor Ort miteinander verbunden. Eine Datenschleuse (s.u.) erhält ggf. einen Anschluss an diesen Switch und einen Anschluss an eine normale Netzwerkdose (oder wird direkt an ein betroffenes einzelnes System angeschlossen).
- Systeme sind über die Etage/Gebäude verteilt, aber über **einen** Switch an die Infrastruktur der TU-Braunschweig angebunden: Es wird ein lokales Vlan auf diesem Switch angelegt, in dem nur diese Geräte miteinander verbunden werden. Eine Datenschleuse (s.u.) wird mit je zwei Datendosen verbunden, von denen eine in das lokalen Vlan, die andere in ein reguläres Vlan geschaltet ist.
- Systeme sind über mehrere Etagen/Gebäude verteilt (und über mehrere Switche an die Infrastruktur der TU-Braunschweig angebunden): Die Geräte können zur Zeit nicht gemeinsam in einem Netz gekapselt werden. Es müssen ggf. mehrere lokale Netze (s.o.) angelegt werden.

Wie kann man den Austausch von Daten zwischen den IT-Systemen ohne Support und der restlichen Welt lösen? (Stichwort "Datenschleuse")

Der Austausch von Daten zwischen den nicht mehr supporteten System und dem Rest der IT ist als kritisch zu bewerten und muss über eine "Datenschleuse" erfolgen, die Kompromittierungen in beide Richtungen ausschließt. D.h. Daten, die von den nicht supporteten Systemen auf regulär betriebene Systeme übertragen werden sollen, müssen vorher zunächst auf dieses System übertragen und nach aktuellem Stand der Technik auf Viren etc. untersucht werden. Gleiches gilt in die andere Richtung.

Solche Datenschleusen können in der Praxis auch Rechner sein, die über zwei Netwerkkarten verfügen, und jeweils mit "einem Bein" im privaten/lokalen Netz mit den nicht supporteten Systemen stehen und mit dem anderen Bein in einem regulären Netz. Dabei muss es sich bei diesem Rechner in jedem Fall um ein vom Hersteller des Betriebssystems noch unterstütztes (jederzeit vollständig gepatchtes) System handeln, dass ebenso über Virenscanner mit jederzeit aktuellen Virensignaturen etc. verfügt und die Daten vor Weiterübertragung in beide Richtungen überprüft. Dieses System darf zudem nicht von außerhalb des Netzes zugreifbar sein (FW-Regeln auf Instituts-Firewall) und muss auch über die lokale Firewall so weit wie möglich geschützt werden.

> Was ausdrücklich **nicht** passieren darf, ist der **Austausch von Daten über Wechselmedien** (USB-Sticks und co.) ohne Überprüfung auf Kompromittierung mit aktuellen Virenscannern etc.

Kann ich dann aus dem "Alt-Netzwerk" z.B auf Netzlaufwerke zugreifen (Isilon)?

Nein. Das darf so nicht umgesetzt werden, weil das den ganzen Aufwand zur Kapselung wieder in Frage stellt. Die Daten sollten immer nur auf einer Datenschleuse (s.o.) abgelegt werden, die z.B. in beiden Welten steht und auf der ein Virenscanner läuft, der die Transferdaten in beide Richtungen prüft.

Habe ich von dort aus Zugang zum Internet?

Nein. Ziel der Kapselung ist die beidseitige Trennung der nicht supporteten Systeme vom Rest der IT.

Kann man mittels Fernwartprogrammen wie Rustdesk (ähnlich Teamviewer, aber Open Source) auf die Altgeräte zugreifen?

Jein. Sinnvoll ist dies eigentlich nur über den Weg der Datenschleuse (s.o.), die dann in jedem Fall mit beiden Netzen verbunden sein muss. Als Software-Lösung können hier z.B. die OpenSource Software https://guacamole.apache.org/ (Linux) in Frage kommen.

Revision #7
Created 30 May 2024 07:49:02 by Tina Strauf
Updated 4 June 2024 05:40:22 by Tina Strauf