Steinbuch Centre for Computing

Leitung: Prof. Dr. Martin Frank
Prof. Dr. Bernhard Neumair
Dr. Martin Nußbaumer
Prof. Dr. Achim Streit

Erstellt von: Junker, Birgit
Erstellt am: 14.05.2021
Geändert von: Junker, Birgit
Geändert am: 18.05.2021

21. IT-Beauftragten Versammlung am 12.05.2021

Termin: 12.05.2021, 9:30 – 11:30 Uhr
Verteiler: IT-Beauftragte am KIT, SCC

Protokoll: https://www.scc.kit.edu/misc/itbv-dokumente/ITBV_Protokoll.2021.05.12.pdf

Präsentation: https://www.scc.kit.edu/misc/itbv-dokumente/ITB-Versammlung_20210512.pdf

Tagesordnung

Top 1 – Begrüßung – Neues aus dem SCC

Herr Lorenz begrüßte die Anwesenden zur 21. IT-Beauftragten Versammlung und ging kurz auf die organisatorischen Änderungen am SCC ein. Frau Brenneisen hat das SCC verlassen. Die stellvertretende Leitung der Abteilung „Informationssysteme für Organisation und betriebliche Ressourcen (IOR)“ hat Herr Martin Hengel übernommen.

Top 2 – Behandlung von Sicherheitslücken in Embedded Systems

Vortragender: Peter Oettig (SCC-SYS)

In seiner Präsentation zeigte Herr Oettig auf, dass an das Internet angebundene eingebettete Systeme häufig Sicherheitslücken aufweisen und damit gern ein Angriffsziel für Hacker sind.
Damit stellen diese Systeme, die vermehrt zum Einsatz kommen, ein Risiko für die IT-Sicherheit am KIT dar. Vertrauliche Daten können in falsche Hände geraten oder andere Systeme können wiederum über ein gehacktes eingebettetes System angegriffen werden.
Desktops und Server sind i.d.R. im Fokus der Administratoren und meist auf einem aktuellen Software-Stand, während eingebettete Systeme gerne vergessen werden. Dazu kommt, dass es meist entweder eine Aktualisierungsmöglichkeiten gibt oder vorhandene Updates nicht automatisiert eingespielt werden.

Wichtig ist, dass sich die Betreiber solcher eingebetteten Systeme über dessen potentielle Anfälligkeit informieren. Ein in den Folien beigefügter Flowchart zeigt das Vorgehen beim Prüfen und Absichern der Geräte auf.

Zudem wies Herr Oettig auf einen Scanner (s. Folien) hin, der im lokalen Netzwerk (in jeder BCD; ein VLAN ist per Definition eine Broadcastdomain (BCD)) zur Prüfung auf anfällige Geräte eingesetzt werden kann.
Eine virtuelle Maschine, auf der der Scanner bereitgestellt wird, um diese für das eigene Institut anzupassen, kann nicht bereitgestellt werden, da die Scanner-SW unter VMWare keine brauchbaren Ergebnisse liefert.
Faustregel: Jede Virtualisierungsschicht verschlechtert das Ergebnis.

Top 3 – Single Sign-On für dezentrale Anwendungen – Authentifizierung mit Shibboleth/SAML und OpenID Connect

Vortragender: Ulrich Weiß (SCC-AMA)

Das SCC stellt die Authentifizierung per SSO (Single Sign-On) für eine große Anzahl an Unternehmensanwendungen und IT-Diensten bereit.
Herr Weiß erläuterte anhand anschaulicher Anwendungsszenarien den Aufbau der eingesetzten Authentifizierungsdienste und ging zudem auf deren technische Umsetzung ein.

Die Dokumentationen zu diesem umfangreichen Thema findet man auf den SCC Webseiten.

- Shibboleth Identity Provider (Shib): https://www.scc.kit.edu/dienste/6921
- OpenID Connect Provider (OIDC): https://www.scc.kit.edu/dienste/openid-connect
- RegApp – Authentifizierungs und Autorisierungs-Infrastruktur (AAI): https://www.scc.kit.edu/dienste/regapp

Weitere Beschreibungen werden sukzessive auf den SCC Webseiten bereitgestellt.

Im Kreis der ITB gab es Fragen zur Abmeldung bei einigen Anwendungen, bei denen kein Logout-Button o.ä. existieren.
Sofern die Anwendung keine Abmeldung selbst auslöst, gibt es zumindest in OIDC ein Account-Portal, über das man sich abmelden kann. In Shibboleth/SAML funktioniert ein Logout bzw. Single-Logout hingegen nur mit Einschränkung, z.B. zentral via https://my.scc.kit.edu/Shibboleth.sso/Logout.

Um die Windows-/Kerberos-Authentifizierung im Firefox zu ermöglichen, muss dort lt. ITB (Dank an Hr. Knieling!) der Schlüssel „network.negotiate-auth.delegation-uris“ in „about:config“ auf „.kit.edu“ gesetzt werden. Voraussetzung ist eine funktionierende Kerberos-Einrichtung (wie z.B. Mitglied in der KIT.edu-Domain).
Angeregt wurde seitens der ITB die Verlängerung der Shib-Sessions auf einen kompletten Arbeitstag, um die erneute Anmeldung, z.B. im SAP-Portal ESS/MSS zum Auschecken, zu vermeiden.

Zur Einbindung eigener Anwendungen bietet das SCC zumindest für Standardanwendungen fertige Konfigurationen und unterstützt hier gern.
Interessierte wenden sich hier bitte an die in Folie 29 der Präsentation genannten Personen.

Top 4 – Backuplösung mobiler Geräte - Update

Vortragende: Doris Ressmann (SCC-SDM)

Wie bereits per SCC-Meldungen und zuvor im IT-Expertenkreis (ITEK) angekündigt kann die Backuplösung mobiler Geräte mit Druva Insync ab dem 20.05.2021 definitiv nicht fortgesetzt werden. Die als Alternative ursprünglich in Frage kommende Software FileCloud hat sich letztendlich als nicht einsetzbar erwiesen. Das SCC wird eine Liste der darüber hinaus untersuchten Backuplösungen erstellen und nachreichen.

Derzeit kann das SCC nur die Backuplösung mit IBM Spectrum Protect (ISP/TSM) anbieten. Frau Ressmann erläuterte die Unterschiede zwischen den beiden Backuplösungen und ging auf die notwendigen Schritte und Randbedingungen zur Umstellung der mobilen Geräte auf die Backuplösung ISP/TSM ein.

Die ITB merkten an, dass IBM Spectrum Protect (ISP/TSM) keine alternative Lösung sei und die Information darüber, dass FileCloud doch nicht angeboten würde, zu spät (später als versprochen lt. Protokoll ITEK vom 24.03.21: https://team.kit.edu/sites/it-expertenkreis/Protokolle/2021_03_24/Protokoll IT-EK 20210324.pdf) an die ITB kommuniziert wurde. Dadurch wären einige ITB tatsächlich in Bedrängnis gekommen, um die Alternative Software auf zahlreichen ihrer betreuten Clients rechtzeitig bis zum 20.5.21 einzurichten oder eine andere Alternative zu realisieren.

Im Nachgang erläuterte Herr Streit noch einmal ausführlich warum zum einen Druva Insync nicht mehr eingesetzt werden kann (Druva Insync ab 21.5.21 nur noch als Cloud-Dienst vom Hersteller nutzbar), zum anderen wie das SCC bei der Auswahl einer Alternative vorgegangen ist und sich letztendlich erst so spät gegen FileCloud entscheiden konnte (Hersteller von FileCloud hatte bis Anfang Mai ein Update zur Beseitigung entscheidender Bugs versprochen, das bis dato nicht verfügbar ist).

Sobald die jetzt aufkommende Unterstützungsleistung des SCC Backup Teams im Rahmen der Umstellung auf ISP nachgelassen hat, wird das Team sich erneut um eine alternative Backuplösung für mobile Geräte bemühen.

Des Weiteren machte Frau Ressmann auf aktuelle Sicherheitslücken beim ISP Client aufmerksam. Aufgrund dieser Sicherheitslücken ist ein Update der ISP Clientsoftware auf Version 8.1.12.0 dringend empfohlen.

Top 5 – Änderungen an IT-Infrastruktur und IT-Diensten

Vortragender: Andreas Lorenz (SCC-ISM)

Es gab in der Vergangenheit eine Reihe an Änderungen am SCC, die in Einzelfolien präsentiert wurden.

- NHR@KIT - Inbetriebnahme HoreKa
- SAP Portal - Umstellung Neues Framework
- Netzwerk-Infrastruktur - KITnet, VPN
- Filesharing und Datenbanken
- Umstellung der KIT-Webserver auf https-only
- Virtueller Rundgang am SCC - www.scc.kit.edu/ueberuns/tour

Das SCC strebt zudem die Umsetzung einer E-Mail-Archivierung an (Wunsch vieler Nutzenden). Weitere Informationen dazu werden im nächsten IT-Expertenkreis (ITEK) folgen.
In ca. 1-2 Monaten wird es zudem eine zentrale Empfehlung für Stockwerksdrucker am KIT geben. Durch eine Authentifizierung über die KIT-Card und der „Follow Me Printing“ Funktion werden die Ziele der Informationssicherheit unterstützt.

Top 6 – Sonstiges / Diskussion

Moderator: Andreas Lorenz (SCC-ISM)

Herr Burgdorf, Informationssicherheitsbeauftragter (ISB) des KIT, rief die ITB dazu auf, insbesondere bei Mitarbeiter*innen und Arbeitsgruppen, die sich mit dem Thema der Corona Pandemie beschäftigen, besonders aufmerksam in Bezug auf die IT-Sicherheit der eingesetzten Systeme und Daten zu sein.
Weiterführende Informationen wurden im Portal des IT-Expertenkreises unter IT-Sicherheitsinformationen eingestellt.