MAßNAHMEN ZUR GEWÄHRLEISTUNG VON INFORMATIONSSICHERHEIT FÜR SAS® 9.4 UMGEBUNGEN

FRANK ROSNER, SOLUTION ARCHITECT
SAS DEUTSCHLAND

AGENDA

- Informationssicherheit
  - Was ist das und warum geht mich das an?
- Wie steht SAS® dazu, welche Maßnahmen gab es und laufen noch?
- Konkret:
  - Warum verwendet SAS® kein Java8?
  - Hotfixes, speziell Java-Hotfixes:
    - Welche Schritte gibt es dabei?
- Nutzen von SAS® 9.4-Sicherheits-Features in eigenen SAS® -Programmen.

ZIELE DES VORTRAGS

- Information über die Sicherheitsmaßnahmen von SAS®.
- Mehr Klarheit über gegenseitige Zusammenhänge.
- Zum Nachdenken anregen:
  - Wie passt das mit meinen Prozessen zusammen?
  - Was brauche ich speziell (noch)?
- Fragen sind erwünscht!

EIN BEISPIEL | WIE ES NICHT LAUFEN SOLLTE

- Einbruch bei Target Ende 2013.
  - Hacker erbeuteten 40 Millionen Kreditkartendaten und 70 Millionen Kundendaten.
  - Im Mai 2014 tritt der CEO Gregg Steinhafel zurück.
- Weckruf für Unternehmen:
  - Erstmalig waren Sicherheitsfragen die primäre Ursache für einen erzwungenen Rücktritt eines CEO.
- Andere Beispiele: Angriffe bei Sony Pictures Entertainment (2014), Stuxnet (2007-2010), RSA SecureID (2011), Kaspersky Lab (2015).

RATIONALER ANSATZ NÖTIG

- Informationssicherheit ist emotional besetzt.
- Abwägen zwischen Risiko und Kosten von Gegen-Maßnahmen nötig.
- Eine(!) wichtige Gegenmaßnahme: „Einspielen von Hotfixen“.
- Objektivierungsmöglichkeiten:
  - Für Seite des Risikos:
    - Was muss geschützt werden?
    - Was ist die konkrete Gefahr?
    - Was sind die Mittel der Angreifer und wie schnell können sie agieren?
  - Für Seite der Gegenmaßnahmen:
    - Welche Gegenmaßnahmen gibt es überhaupt (noch)?
    - Wie teuer sind sie im einzelnen?
    - Was genau können sie verhindern?

GRUNDWERTE DER INFORMATIONS-SICHERHEIT

AUS: „LEITFADEN INFORMATIONSSICHERHEIT DES BUNDESAMTES FÜR SICHERHEIT IN DER „INFORMATIONSTECHNIK (BSI)

- **Vertraulichkeit**
  - Vertrauliche Informationen müssen vor unbefugter Preisgabe geschützt werden.
- **Verfügbarkeit**
  - Dem Benutzer stehen Dienstleistungen, Funktionen eines IT-Systems oder auch Informationen zum geforderten Zeitpunkt zur Verfügung.
- **Integrität**
  - Die Daten sind vollständig und unverändert. Der Begriff „Information“ wird in der Informationstechnik für „Daten“ verwendet, denen je nach Zusammenhang bestimmte Attribute wie z. B. Autor oder Zeitpunkt der Erstellung zugeordnet werden können. Der **Verlust der Integrität** von Informationen kann daher bedeuten, dass diese unerlaubt verändert wurden oder Angaben zum Autor verfälscht wurden oder der Zeitpunkt der Erstellung manipuliert wurde.

GRUNDSÄTZE DER INFORMATIONSSICHERHEIT

DATEN-VERTRAULICHKEIT

- „data-at-rest“
- „data-in-motion“

VERFÜGBARKEIT

- System uptime
- Skalierbarkeit
- Denial of Service

INTEGRITÄT

- Daten
- Programme
- Ausführung

AUTHENTIFIZIERUNG

- Sicheres credential management
- Sichere Integration mit externen Identity-Providern
- Identitäts-Propagierung

AUDITING

- Systemkonfiguration
- Zugriffskontrolle
- Zustandsänderungen (+/-)
- End-to-end audit trail
- Anonymisierungsfähigkeit

AUTORISIERUNG

- „Feinkörnige“ Zugriffskontrolle
- Regel- und Rollenbasierung

„VULNERABILITIES“

= SCHWACHSTELLEN, VERWUNDBARKEIT, ANGREIFBARKEIT, VULNERABILITÄTEN, SICHERHEITSLÜCKEN

- Wie entstehen sie?
  - Software-Bugs (die für Angreifer ausnutzbar sind),
  - Schwächen in der Konfiguration (z.B. auch Rechte-Konfiguration).
- Komplexe Softwaresysteme.
- Sicherheits-Hotfixe sind Reaktion auf (das Veröffentlichen von) Sicherheitslücken.
- Jede Veröffentlichung einer Schwachstelle ist positiv zu werten, weil (nur) dadurch Schutzmaßnahmen möglich sind: eine nicht-veröffentlichte Sicherheitslücke hilft nur Angreifern .

DER ZEITFAKTOR UND DER SOFTWARE-UPDATE-ZYKLUS

- Eine nicht erkannte (= nicht veröffentlichte) Vulnerabilität ist nur durch die Angreifer nutzbar, die sie kennen und die Mittel entwickelt haben, sie auszunutzen.
- Mit der Veröffentlichung steigt die Gefahr für alle, die keine Gegenmaßnahmen ergreifen:
  - Die anderen Angreifer erhalten jetzt die Information, dass eine Lücke besteht und können Angriffsmittel erstellen, d.h. die Anzahl der potentiellen Angreifer wächst.
  - Der Schaden, den die neuen Angreifer anrichten können, konzentriert sich auf die Systeme ohne Patches (oder andere Gegenmaßnahmen).
- Diese erhöhte Gefahr führt zum „Zwang“ von zeitnahen Patches und hat damit Auswirkungen auf den (normalen) Software-Update-Zyklus.

„ERGÄNZUNGEN“ ZU FIXES

- Konsequentes Einschränken der Rechte von Diensten mit Betriebssystem-Mitteln (siehe z.B. SE Linux, AppArmour, cgroups),
- Umfangreiches Auditing,
- Intrusion Detection Systeme,
- Juristisches Vorgehen (funktioniert nicht mit allen Angreifertypen).

INFORMATIONSSICHERHEIT BEI SAS®

ÜBERBLICK ÜBER DIE MAßNAHMEN

- Software Security Framework:
  - Integration von Best Practices bzgl. Informationssicherheit in den Life cycle von Entwicklung und Support.
- Product Security Incident Response Team:
  - Gewährleistung eines zeitnahen Schließens von Sicherheitslücken.
- Offene Kommunikation über Informationssicherheit:
  - Information über Sicherheitsprobleme.

SAS® SOFTWARE SECURITY FRAMEWORK

- Beschrieben im White Paper: https://www.sas.com/content/dam/SAS/en_us/doc/whitepaper1/sas-software-security-framework-107607.pdf.
- Grundaussage: „SAS® is committed to delivering SAS® products that meet and exceed the expectations of our customers”.
- Abschnitte:
  - Education,
  - Secure Architecture and Design,
  - Secure Development Standards,
  - Security Testing and Validation,
  - SAS® Product Security Response and Remediation.

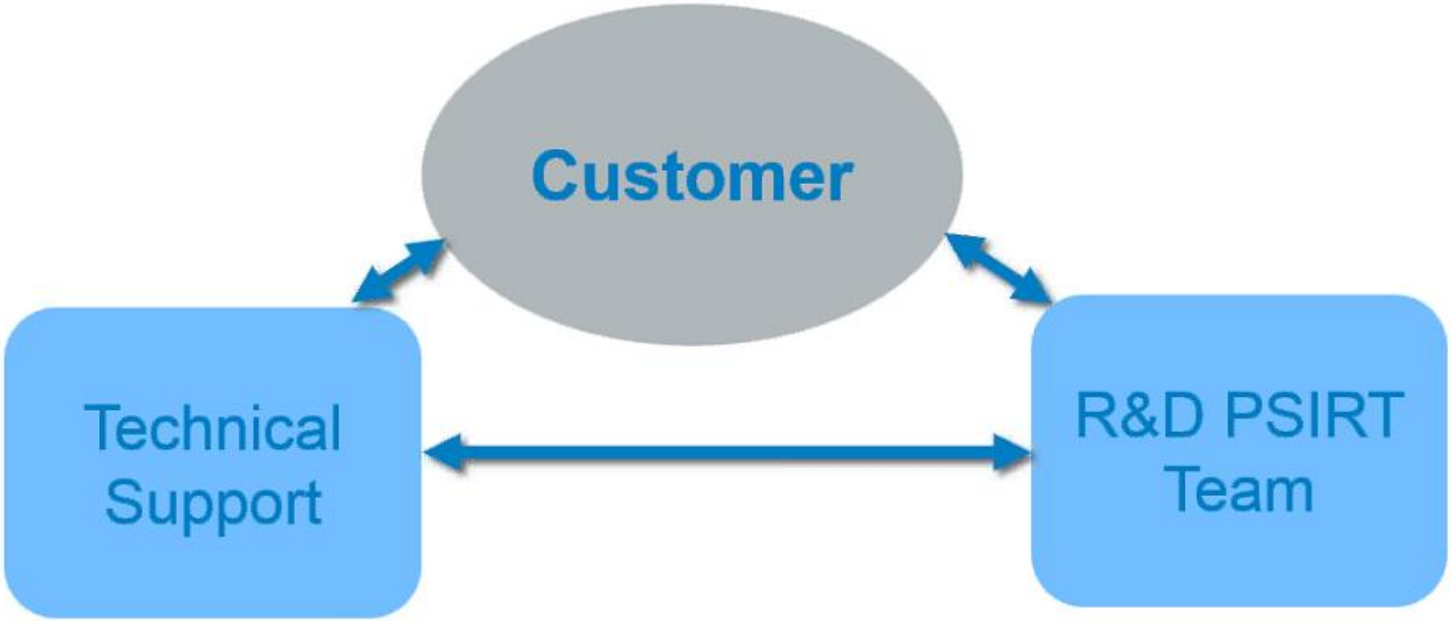
ZENTRALE ANSPRECHSTELLE: TECH SUPPORT

- Security-Fragen laufen über Tech Support.
- Außergewöhnliche Sicherheitslücken erscheinen im „Security Bulletin“: http://support.sas.com/security/alerts.html.
- Der heutige Stand sieht so aus:

Security Bulletins from SAS

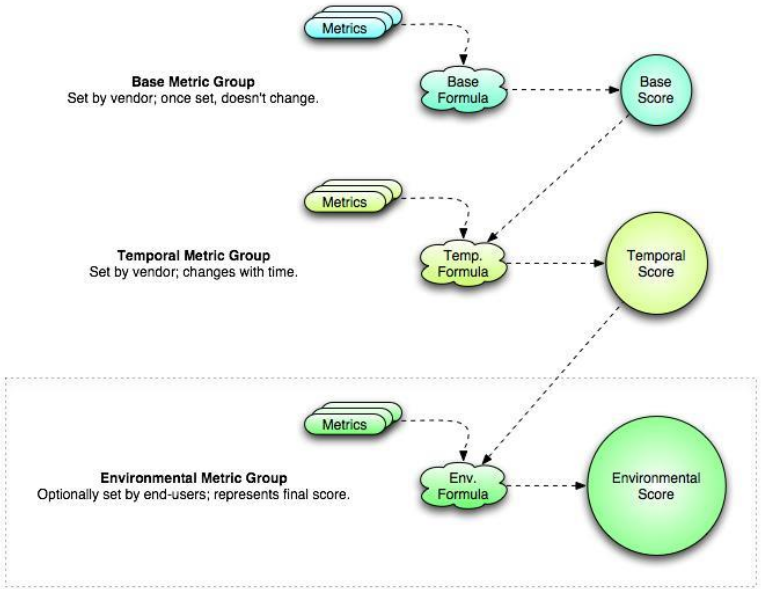
- SAS Statement Regarding the GHOST Vulnerability (March 31, 2015)
- SAS Statement Regarding the FREAK and SKIP-TLS Vulnerabilities (March 4, 2015)
- Daily Report Emails (November 13, 2014)
- SAS Statement Regarding POODLE SSL (October 28, 2014)
- SAS Statement Regarding the Bash Vulnerability (October 16, 2014)
- Notice to SAS Migration Utility Users (October 8, 2014)
- SAS Statement Regarding Heartbleed (April 17, 2014)

PRODUCT SECURITY INCIDENT RESPONSE TEAM



COMMON VULNERABILITY SCORING SYSTEM (CVSS)

- Von „FIRST“ (Forum of Incident Response and Security Teams), siehe https://www.first.org/cvss.
- Es gibt einen „calculator“.
- Mittel zur klareren Einschätzung der Sicherheitslücken („Objektivierung des Gefahrenpotentials“).



DISKUSSION DER BESTANDTEILE VON SAS® SOFTWARE UND DEREN SUPPORT-POLICY BEI VULNERABILITIES

SAS® GUI-Anwendungen

Visual Analytics, CI Studio

„Embedded“ Software

Gemfire, Hyperic

SAS® Infrastruktur-Komponenten

„sas.exe“, sas.xxx.jar

Open Source

OpenSSL, Apache commons

Quasi-open source mit optionalem Vendor-Support

Java (Oracle/IBM)

KRITISCHE PUNKTE, DIE ZU EINER VERLANGSAMUNG DER BEREITSTELLUNG VON PATCHES FÜHREN

- **Gegenseitige Versions-Abhängigkeiten:**
  - Das Erhöhen der Version einer Komponente (z.B. wegen einer erkannten Vulnerability) kann zu Fehlern bei anderen Komponenten führen.
  - Nach solchen Änderungen muss getestet und die neu erkannten Fehler müssten gefixt werden.
- Bestimmte Komponenten ändern sich ohne eigene Kontrolle (und führen zu ähnlichen Effekten):
  - Browser-Updates,
  - Windows-Updates,
  - Java-Updates (für die GUI-Teile in Sun‘s Java 1.7).
- Bei Open Source-Komponenten gelingt es nicht automatisch, sie „normal“ zu patchen (keine Verantwortlichkeit), teilweise mussten Patches zurückportiert werden.

SAS UND JAVA 8

- Es gab 2014 umfangreiche Tests, sowohl zum Austauschen von Java7-Versionen als auch zum Wechsel auf Java8.
- Das führte zum Eröffnen von Tickets, von denen einige gelöst wurden, aber insgesamt zur Entscheidung führten, für SAS9.4 auf Java7 zu bleiben (und dort die Java7-Minor-Version nachzuführen).
- Kritische Punkte:
  - Java Web Start. AspectJ/BCEL.
  - Java auf AIX und HP-UX (2014 noch nicht verfügbar).
  - Hyperic-Technologie im Environment Manager.
  - Schiere Menge der nötigen Umstellungen.
- Laufender Stand: jre1.7.0_85:
  - Entweder durch Installation von SAS9.4M3 oder (für vorige Versionen) durch Einspielen über Hotfix.

PATCH MANAGEMENT BEI SAS®

AM BEISPIEL DER JAVA UPDATES

GRUNDSÄTZLICHES ZU JAVA7-UPDATES

- http://support.sas.com/resources/thirdpartysupport/Java7Updates.html beschreibt die Java7-Update-Policy:
  - SAS® will continue to use and support a Java 7 Java Runtime Environment (JRE) for SAS® 9.4 and SAS® 9.3 deployments and a Java 7 Java Development Kit (JDK) for the SAS® 9.3 middle tier. SAS® will provide updates for critical security issues associated with the Java 7 JRE and JDK in accordance with our technical support and security policies. **SAS® has engaged with Oracle to extend support for Java 7 at no incremental cost to customers**. We anticipate that updates will be available quarterly, aligning with Oracle's Critical Patch Update schedule.

WAS HEIßT DAS KONKRET?

- SAS® stellt (sonst nicht öffentlich erhältliche) JRE/JDK-Versionen von Oracle als SAS® Hotfixe bereit, diese ersetzen die bisherige „sas private jre“ (in SAS® 9.4), wenn sie installiert werden.
- Die Usage Note 56203 (http://support.sas.com/kb/56/203.html) beschreibt den Prozess
- Beim Herunterladen kann eine „license validation“ erfolgen.
- Für HP/UX Itanium und AIX stehen die jeweils frischesten Versionen bereit, deren Versionsstand kann anders sein als bei den Oracle-Versionen für die anderen Plattformen.
- Die JDK‘s (für SAS® 9.3) müssen nur ausgepackt zu werden, die SAS® 9.4-JRE-Versionen werden als Hotfixe eingespielt.

EINSPIELEN ALS HOTFIX (U100001)

- Mit dem SAS® Deployment Manager (SDM).
- Alle SAS® -Prozesse (auch Spawner) müssen beendet sein, wenn der Hotfix eingespielt wird.
- Weil die JRE einem Update unterzogen wird, der SDM aber die JRE benutzt, gibt es einen Restart-Prompt.
- Es gibt einen Post-Installation-Step: Kopieren von JSSECACERTS (betrifft SAS® 9.4 M3).

ÄNDERUNG BEI SAS® 9.4 (BETRIFFT SSL)

- Vor SAS® 9.4 M3 wurden Zertifikate für die JRE in „cacerts“-Datei eingetragen, in SAS9.4 M3 verlagerte sich das auf JSSECACERTS.
- Der SDM hat jetzt einen eigenen Punkt zum Hinzufügen von Zertifikaten, dabei werden auch Abhängigkeiten der Zertifikate untereinander berücksichtigt.
- Die Konfiguration für SSL-Einsatz im SAS® Web Server wurde vereinfacht.
- Neues Verzeichnis im <SASHOME>-Bereich:
  SASSecurityCertificateFramework

ZEITABLÄUFE BEIM LETZTEN JAVA-UPDATE

- Auslöser von 1.7.0_85 waren über 20 Sicherheitslücken (siehe http://www.oracle.com/technetwork/topics/security/cpujul2015-2367936.html#AppendixJAVA).
- Oracle brachte das Update am 14. Juli 2015 heraus (laut derselben URL).
- Veröffentlichung des Hotfixes auf support.sas.com: 16. Juli 2015 (created), 1. August (modified).

ZEITABLAUF BEI LETZTEM OPENSSL-UPDATE

- Quelle: http://support.sas.com/kb/56/481.html.
- Dort Hinweis auf Veröffentlichungstermin:
  OpenSSL advisories through 9th July 2015.
- **Publikation des Hotfixes (betreffen mehrere Midtier-Komponenten, nicht nur den SAS® Web Server): 24.08.2015.**

NUTZEN VON SAS® 9.4-SICHERHEITS-FEATURES

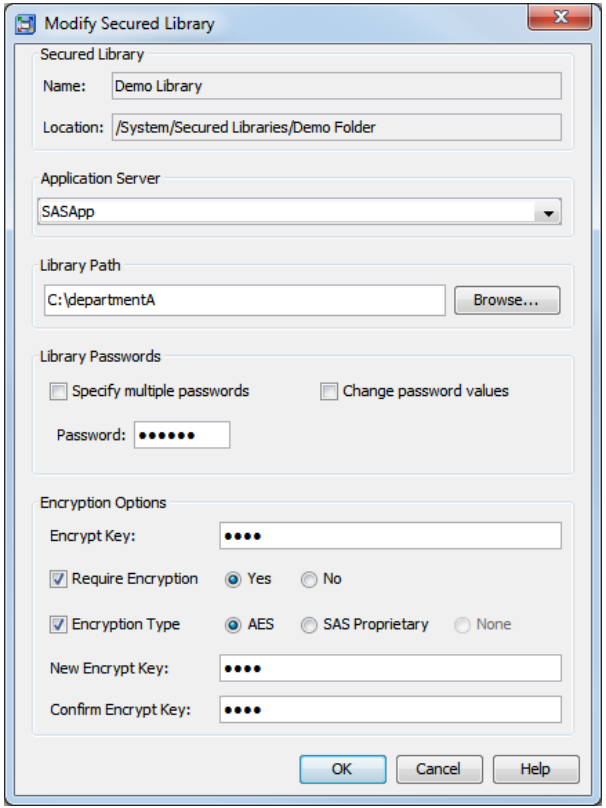
IN EIGENEN SAS® -PROGRAMMEN

SINGLE SIGNON, IWA

- Kennwörter lassen sich nicht nur verringern, sondern auch eliminieren.
- Eine sichere Art, dies zu tun, ist der Industriestandard Kerberos (IWA, SPNEGO) oder token-basierte Standards (z.B. CAS).
- Steigerung der Endbenutzer-Akzeptanz!
  - Kein Eingeben von Kennwörtern.
  - Kein Vergessen von Kennwörtern.
  - Kein regelmäßiges Wechseln von Kennwörtern.

SAS® -SPEZIFIKA: BASE SAS®

- Object Spawner/Connect Spawner sind sicherheitskritisch:
  - Erhöhte Rechte („Delegation“)
- AES-Verschlüsselung auf SAS-Seite
  - Siehe auch REQUIRE_ENCRYPTION Option einer Metadata bound library.
- Einsatz des „lockdown“-Modus.



SAS® -SPEZIFIKA: PROGRAMMIEREN

- Keine Kennwörter in Programmen:
  - Varianten der Programmierung wählen, wo Kennwörter „außerhalb“ liegen.
  - Prüfen, ob es eine Implementierungsvariante ohne Kennwörter gibt.
- Stored Processes können beliebige HTML erzeugen (und dabei Javascript anziehen):
  - Scannen auf Schwachstellen erwägen.
  - Penetrationstests.

SAS® -SPEZIFIKA: MOBILE CLIENTS

- White- und Blacklists für Clients.
- Transport-Verschlüsselung.
- Software-Container:
  - Good technologies und Mocana werden unterstützt

SAS® -SPEZIFIKA: SAS® MIDTIER

- **SAS® Midtier: 3 verschiedene GUI-Typen:**
  - „klassisch“ (HTML4, größtenteils serverseitig generiert)
  - Flash-Clients
  - HTML5
- **Transportsecurity:** SDW unterstützt Konfiguration auf SSL, weitere Erhöhungen der Sicherheit führen zu manuellen Anpassungen.
- **Falls in DMZ: Einsatz des SAS® Web Servers prüfen:**
  - Alternative 1: reverse security proxy (WebSEAL, Siteminder,…).
  - Alternative 2: aktueller Apache.
- Authentication von Webanwendungen ist oft unternehmensspezifisch und sicherheitsrelevant.

SAS® -SPEZIFIKA: PLATTFORM

- FIPS-compliance erwägen („Federal Information Processing Standard “).
- Sicherheit durch Auditing:
  - Eingebautes Auditing in der Plattform.
  - Custom auditing ergänzen (z.B. über ARM-Logging).
  - Verstärktes Auditing ist ab Herbst 2014 im Environment Manager eingebaut worden (entspricht SAS® Audit, Performance and Measurement Package / EBIAPM).

SUMMARY

- SAS® kümmert sich um Sicherheit und setzt dabei auf Industriestandards (z.B. CVSS).
- Zeitnahe Hotfixes sind ein sehr wichtiges, aber nicht das einzige Mittel, um Sicherheitsprobleme zu entschärfen.
- Auf der Ebene der SAS® -Programmierung und -Konfiguration sollten eigene Maßnahmen die „eingebaute“ Sicherheit flankieren (z.B. weitgehende Vermeidung von Kennwörtern).

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT!