SAP ALM
SECURITY OPTIMIZATION SERVICE

Veerle Maas, Frank Muris, Erwan Vossen

9 November 2021

VOORSTELLEN

Veerle Maas

Secretaris ALM

secretarisalm@vnsg.nl

VOORSTELLEN

Frank Muris

Voorzitter SAP ALM

voorzitteralm@vnsg.nl

VOORSTELLEN

Erwan Vossen

SAP ALM Consultant

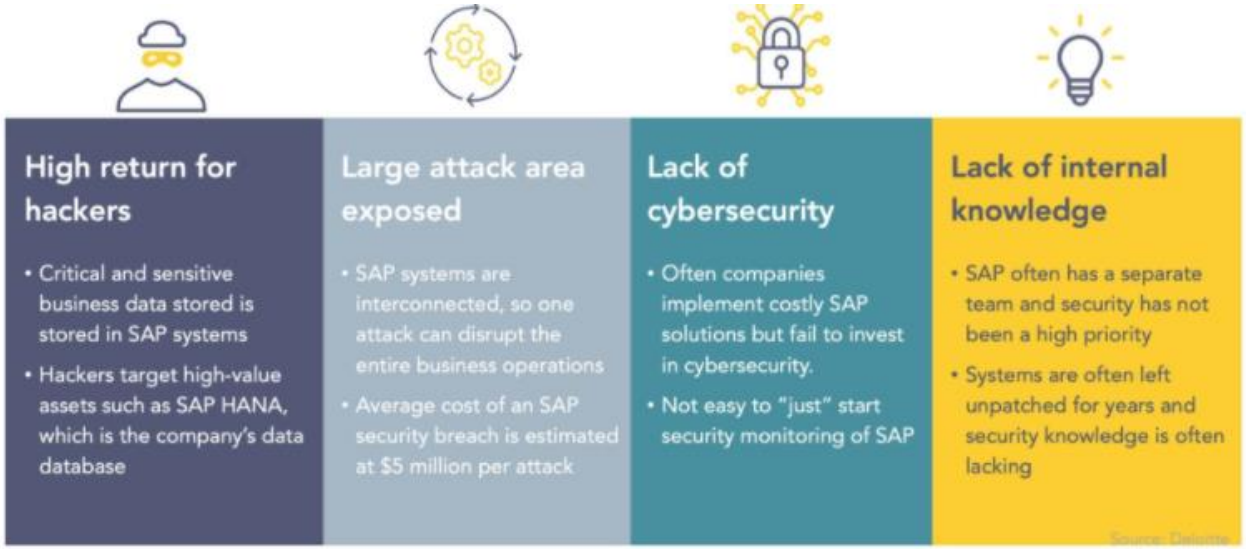
Erwan.Vossen@simac.com

INHOUDSOPGAVE

1. SAP Security
2. Security Optimization Service
3. Demo
4. Prerequisites
5. Conclusie

SAP SECURITY – EXTERNE BEDREIGINGEN

- Aanval op SAP-systemen kan verwoestende impact hebben op een bedrijf – zowel financiële als reputatieschade
- Behouden van vertrouwelijkheid, beschikbaarheid en integriteit van SAP-systemen is daarom essentieel
- Ineffectieve identificatie van mogelijke beveiligingsproblemen kan schadelijk zijn



SAP SECURITY
- INTERNE BEDREIGINGEN

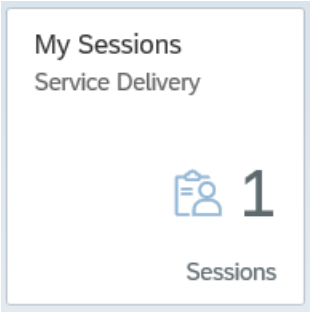
- Social engineering
- Onvoldoende overzicht over verantwoordelijkheden en activiteiten van groot belang voor interne veiligheid
- Onbeperkte bevoegdheden voor werknemers kan onbedoelde negatieve gevolgen met zich meebrengen
  - "You can have the best technical systems in place, but they're not effective if people aren't educated about the risks" – Mike Maddison (Deloitte UK)

SAP SECURITY - TOOLS

Solution Manager Security Tools

- Early Watch Alert (EWA)
  - Monitoring service voor essentiële administratieve aspecten van een SAP systeem
  - Technische onderwerpen bv. Database, Hardware etc.

- Security Optimization Service (SOS)
  - Snapshot van beveiligingszaken in een systeem
  - Identificeert beveiligingsproblemen en biedt oplossingen



SECURITY OPTIMIZATION SERVICE

Security Optimization Services onderwerpen:

- Authentication
- Basis Administration & Basis Authorizations
- Change Management
- User Authorization
- Web Application Server
- Human Resources
- SAP HANA Database

SECURITY OPTIMIZATION SERVICE

- Uitgebreide ondersteuningsservice die kritische beveiligingsaspecten (e.g. autorisaties, RFC's) analyseert op basis van een Questionnaire.

- Doelstellingen van de Security Optimization Service:
  - Analyseren van de technische configuratie van SAP systemen op het gebied van security
  - Documenteren van kwetsbaarheden, gedetecteerd door SAP
  - Aanbevelingen / SAP Recommendations om veiligheidsrisico's te mitigeren

SECURITY OPTIMIZATION SERVICE - VOORDELEN & NADELEN

Voordelen

- Lager risico op systeeminbraak en kostbare downtime wordt verminderd
- Vertrouwelijkheid van bedrijfsgegevens verhoogd
- Authenticiteit van Users is gewaarborgd
- Flexibiliteit m.b.t. de Questionnaire

Nadelen

- Beperkt inzicht in het Segregation of Duties (SoD) deel
- SOS dekt niet alles af
- Niet helemaal out-of-the-box zoals een EWA

SECURITY OPTIMIZATION SERVICE - VOORBEELDEN

4.2.3 Interval for Logon with Productive Password is Too Long (AU081)

Parameter: login/password_max_idle_productive

Rating	Instance	Current Value	Recommended Value
!	All instances	0	> 0

Evaluated Risk - Medium As of SAP NetWeaver 7.00, SAP supports this parameter to encourage your users to create more secure passwords.

> **Recommendation:** Activate profile parameter login/password_max_idle_productive.
> This parameter specifies the maximum period for which a productive password (a password chosen by the user) remains valid if it is not used. After this period has expired, the password can no longer be used for authentication purposes.
> For more information, see:
> SAP Note 327917 - New user types as of Release 4.6C SAP Note 862989 - New password rules as of SAP NetWeaver 2004s (NW ABAP 7.0) Online Help – Profile Parameters for Logon and Password (Login Parameters)

4.2.4 Interval for Password Change is too Long (0127)

Parameter: login/password_expiration_time

Rating	Instance	Current Value	Recommended Value
!	All instances	0	30

Evaluated Risk - High You are currently using a password change interval of more than 120, or you have deactivated this option completely.

> **Recommendation:** Change the profile parameter login/password_expiration_time to 30 (or at least not higher than 60, and definitely not to 0 (disabled)).

SECURITY OPTIMIZATION SERVICE - VOORBEELDEN

7.4 Role & Authorization Management

7.4.1 Users are Authorized to Maintain Roles Directly in the Production System (0072)

Roles, profiles, and authorizations must always be changed in the development system. Therefore, authorizations for role and authorization maintenance do not need to be assigned in the productive system at all.

Client	User	Type	Last Name	First Name	Department	User Group
001	BPMON	A	BPMON			
001	DEMO	A	Mol	Dennie		
001	SA_ADM_SMP	A	SA_ADM_SMP			
001	SM_ADMIN_SMP	S	Solman Admin			
001	SM_TECH_ADM	B	SM_TECH_ADM			
001	Count:	5	[7%]			

Evaluated Risk - High

Recommendation: Use the Profile Generator (PFCG) to correct roles, or transactions SU02 (Maintain Profiles) and SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization information system (SUIM) to check the results. For this check, we recommend that you examine the roles or profiles that include the authorization objects listed below.

Authorization objects: Object 1: S_TCODE with TCD=PFCG [and all relevant parameter transactions]
Object 2: S_USER_AGR with ACTVT=01 (create) or ACTVT=02 (change)

	Users are Authorized to Maintain Roles Directly in the Production System (0072)	

SECURITY OPTIMIZATION SERVICE

Demo – Security Optimization Service

PREREQUISITES

SAP Solution Manager System Prerequisites

- Basic Configuration (SOLMAN_SETUP)
- Tenminste de volgende rollen:
  - SAP_SMWORK_BASIC
  - SAP_SMWORK_SERVICE_DEV
  - SAP_SM_SOLUTION_ALL
- Bevoegdheid voor transactie AGS_UPDATE

Managed System Prerequisites

- Transactie SDCCN geconfigureerd
- Bevoegdheden voor Data Collector ST14
  - S_BTCH_JOB (aftrappen van job)
- Autorisatierol:
  - SAP_SECURITY_OPTIMIZATION

CONCLUSIE

Security Optimization Service

- Proactieve aanpak m.b.t. SAP Security
- Draagt bij aan het Security Audit proces
- SAP Best Practice – zoals EWA, SOS etc.
- Goede investering

LINKS

Documentatie

- https://blogs.sap.com/2020/06/17/introduction-to-security-optimization-service-sos-security-health-check-report/
- https://support.sap.com/en/offerings-programs/support-services/security-optimization-services-portfolio.html
- https://launchpad.support.sap.com/#/notes/1484124
- https://launchpad.support.sap.com/#/notes/696478

MEER WETEN OVER SECURITY?

Meld je dan alvast aan voor de volgende bijeenkomst van de focusgroep ALM:

Security met Protect4S

19 januari 2022 – Online sessie