SAST

Bezpieczeństwo SAP

Wyzwania przez kontekst techniczny i biznesowy

2020-06-24

Tomasz Jurgielewicz

Head of Security Development

SAP „out of the box” – czy jest bezpiecznie?

SAST

Konfiguracja

- Parametryzacja - Klient
- Rozwój systemu niezależny od producenta
- SAP regularnie dostarcza noty bezpieczeństwa (łaty), ich wdrożenie - Klient

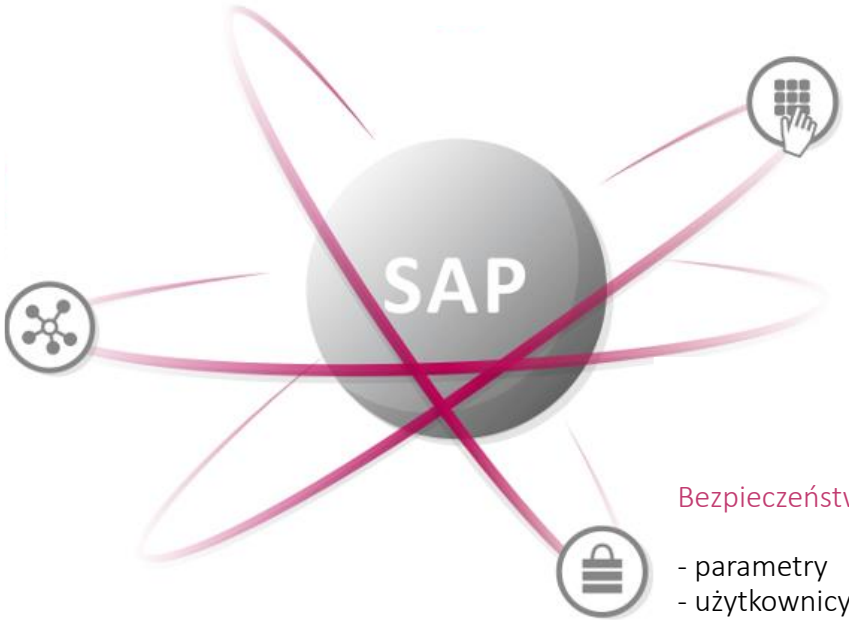
Autoryzacje

- Podczas wdrożeń koncepcja autoryzacji jest często pomijana
- Standardowa praca na dostarczonych rolach i profilach.
- Zbyt szerokie uprawnienia (wykorzystanie średnio 10%)
- Konflikty uprawnień i krytyczne dostępy

Monitoring

- Standardowe narzędzia SIEM nie posiadają wzorców kontrolnych SAP, przez co SAP jest martwym punktem dla ataków
- Mnogość źródeł logów SAP
- Brak wiedzy specjalistycznej do SAP Security

Wyzwania bezpieczeństwa SAP



Autoryzacje i użytkownicy

- dostępy krytyczne
- konflikty uprawnień (SoD)
- krytyczne transakcje
- zarządzanie rolami
- pobieranie danych

Security Intelligence

- real-time monitoring
- SIEM
- zdarzenia ryzykowne
- procesy GRC
- kompensacja, kontrola

Bezpieczeństwo techniczne

- parametry
- użytkownicy techniczni
- podatności

Kompleksowe bezpieczeństwo SAP

Bezpieczeństwo – autoryzacje SAP

Wniosek o autoryzacje

↓

Akceptacja

↓

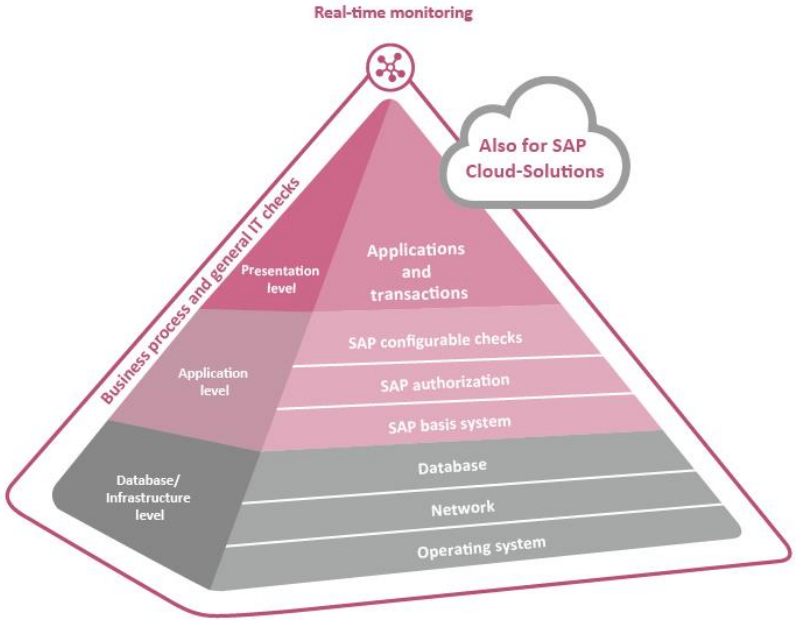
Realizacja

Reguły → Weryfikacja SoD Real-time ← matryca SoD

OK / nie OK

Dostępy uprzywilejowane

Cybesecurity – wszystkie poziomy



Konflikty uprawnień (1)

Funkcja	Ryzyko	Transakcje
Zarządzanie danymi podstawowymi dostawców	Utworzenie nieistniejącego dostawcy	FK01 / XK01
	+	
Fakturowanie towarów przychodzących	Wysłanie fikcyjnej faktury	FB60 / FB65 / FB01 / F-53
	=	
Zarządzanie danymi podstawowymi ORAZ Dane transakcyjne	Ryzyko wysłania faktury dla fikcyjnego dostawcy Wypłynięcie pieniędzy z tytułu rozliczenia faktury	(FK01 / XK01) + (FB60 / FB65 / FB01 / F-53)

Konflikty uprawnień (2)

Obszar	Opis konfliktu	Przykładowe transakcje konfliktowe
SD	Możliwość wprowadzenia dokumentów sprzedaży i obniżenia cen celem osiągnięcia korzyści finansowych dla użytkownika, który może **edytować fikcyjnych dostawców i inicjować zakupy na danego dostawcę**	VA01/VA02/WCS0 + Np.: V32/V32/V33/V35
FI	Uprawnienia do otwierania/zamykania okresów księgowania i do księgowania dokumentów na poprzednie okresy celem zatuszowania nieautoryzowanych zaksięgowań. **Zaksięgowania mogą być wykonywane na fikcyjne konta KG oraz zapisywane są niepoprawne podatki i kursy walut** po upłynięciu danego miesiąca lub roku celem ukrycia innych zaksięgowań.	F04N/F05N/F06N + PERIODES/PERIODES_NAM
HR/PY	Wprowadzenie nieautoryzowanych płatności i realizacja salda rachunku bankowego. Ryzyko wprowadzenia **nieautoryzowanej płatności i potwierdzenia salda bankowego przez tą samą osobę**.	Np.:F-18/F-46/F-58_K + Np.: FEBA/FF.5/FF/4/FF/5

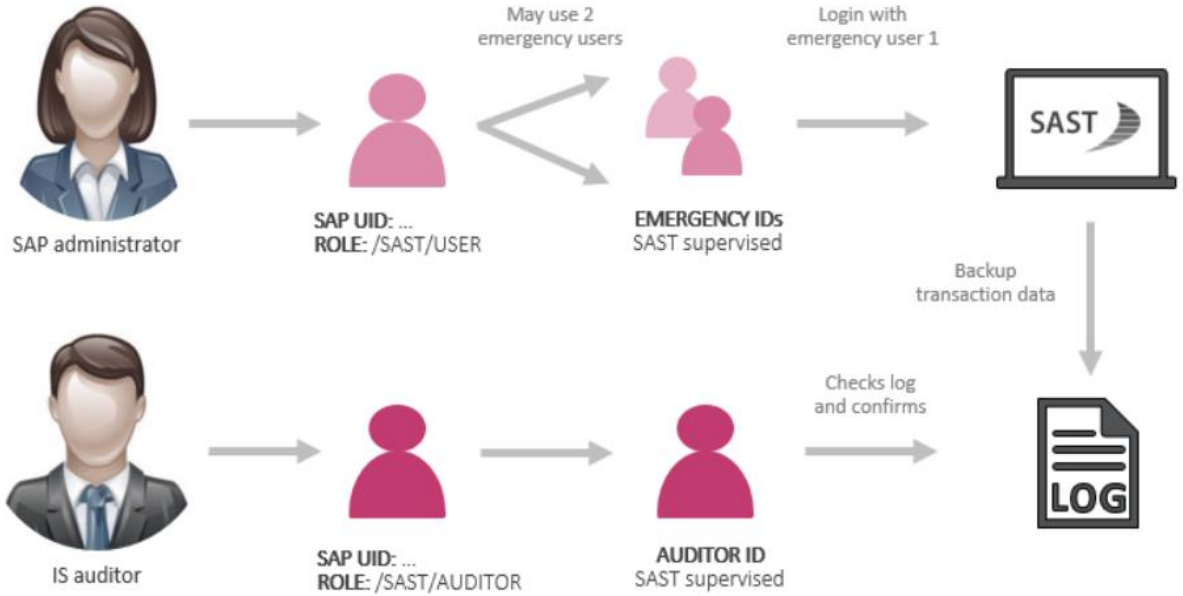
Weryfikacja obszarów technicznych

- SAP NetWeaver specific (XI, Solution Manager)
- JAVA settings
- ITS configuration
- BW specific
- Module specific > FI/CO > HR
- Users and permissions
- NetWeaver internet framework
- Database also SAP HANA DB
- Operating system
- System / Instance parameter

- RFC/Gateway
- LDAP settings
- TMS configuration
- Critical ABAB´s, functions and transactions
- Checksum on files (SAP executables)
- Source Code Scan for critical ABAB statements
- Standard passwords
- Audit firecall users
- Audit SAP standard user

Krytyczne dostępy

„Krytyczny dostęp” to uprawnienia pozwalające na np. prace developerskie ale również fraud lub destabilizacje.



Docelowo – brak krytycznych dostępów na systemie produkcyjnym, dostępy ściśle kontrolowane

Bezpieczeństwo SAP – źródła ataków

Użytkownik biznesowy

Administrator

Środowisko SAP

- Konflikty uprawnień
- Zbyt duże autoryzacje
- Niebezpieczna konfiguracja
- Poprawki (patche)

Możliwe ryzyka

- Oszustwo (defraudacja)
- Błędy
- Podatności
- Utrata kontroli

SAST

- Procesy GRC w SAP
- Monitorowanie krytycznych pobrań
- Manipulacje na użytkownikach
- Scenariusze ataków

Wyzwania i problemy w analizie logów

- **SAP Security Audit Log ABAP**
  Nieczytelne dane: zmiana autoryzacji użytkownika –> jakie role/profile zostały zmienione i przez kogo? Błędna klasyfikacja zdarzeń: Logon ok dla SAP* (zielone), niepoprawne logowanie zwykłego użytkownika (czerwone)

- **Zmiany dokumentów i tabel w SAP – logowanie zmian**
  Niska wydajność, jeśli logowane zmiany dokumentów nie są archiwizowane na czas.

- **SAP System Log**
  Nadpisywanie.

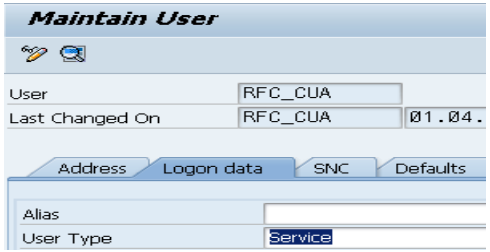
- **Windows/UniX Logs**
  Wymagane autoryzacje root do odczytu danych z logów.

- **Logi baz danych**
  Nieczytelne logi Microsoft SQL.

- **SAP Router Logs / SAP Gateway / HTTP Logs**
  Brak wbudowanej funkcjonalności powielającej syslogi.

Scenariusz ataku – eskalacja uprawnień (user morphing) (1)

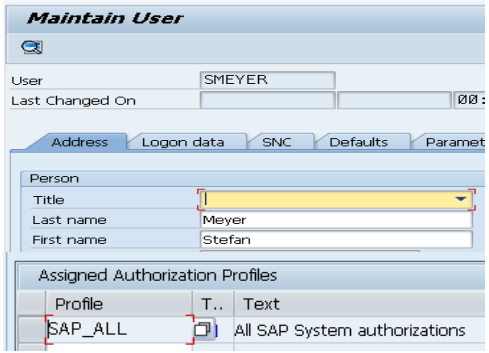
Zmiana typu użytkownika na SERVICE



Logowanie do SAP

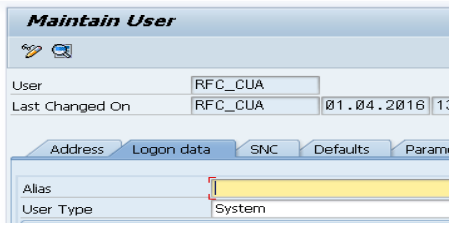
Uruchomienie SU01 do stworzenia użytkownika BACKDOOR

Utworzenie użytkownika BACKDOOR



„Sprzątanie”

Ponowna zmiana użytkownika



Scenariusz ataku – eskalacja uprawnień (user morphing) (2)

SAST

SAP Security Audit Log
nie pokazuje PRAWDZIWYCH krytycznych zdarzeń.

User Name	Terminal	TCode	Security Audit Log message text
RKEMPF	pc-1234	/SAST/SIM_	User Logoff
RKEMPF	pc-1234	SU01	Transaction SU01 Started
RKEMPF	pc-1234	SU01	User Master Record RFC_CUA Changed
RKEMPF	pc-1234	SU01	User Master Record RFC_CUA Changed
RFC_CUA	pc-1234	SESSION_M	Logon Successful (Type=A)
RKEMPF	pc-1234	SESSION_M	Logon Successful (Type=A)
RKEMPF	pc-1234	SU01	Transaction SU01 Started
RKEMPF	pc-1234	SU01	User Master Record RFC_CUA Changed
RKEMPF	pc-1234	SESSION_M	User Logoff
RFC_CUA	pc-1234	SESSION_M	Logon Successful (Type=A)
RFC_CUA	pc-1234	SU01	Transaction SU01 Started
RFC_CUA	pc-1234	SU01	User SMEYER Created
RFC_CUA	pc-1234	SU01	Transaction SU01 Started
RFC_CUA	pc-1234	SU01	User Master Record RFC_CUA Changed
RFC_CUA	pc-1234	SM20	Transaction SM20 Started

Brak informacji na przykład o SAP_ALL

Brak informacji o krytycznych zdarzeniach

Narzędzie do weryfikacji zdarzeń
SAP SIEM

SAST Security Radar (Events) (70)

Exce...	EventID	Severity	Log Line	User Name
	USER_CHANGE	8	UserID: RFC_CUA has changed own user master record	RFC_CUA
	SECLOG_CRIT	10	User Master Record RFC_CUA Changed	RFC_CUA
	USER_PROFILE	9	Auth. profile assigned: User : SMEYER Profil: SAP_ALL by user: RFC_CUA	RFC_CUA
	SECLOG_AU_1	10	Logon Successful (Type=A)	RFC_CUA
	LOG_CRIT	10	User Master Record RFC_CUA Changed	RKEMPF
	LOG_AU_1	10	Logon Successful (Type=A)	RFC_CUA
	LOG_CRIT	10	User Master Record RFC_CUA Changed	RKEMPF

Podejrzane:
RFC zalogowany w trybie dialog

Nowy użytkownik z krytycznymi dostępami

Zespół SOC poinformowany o krytycznych zdarzeniach

SAP Security w liczbach

SAST

over 1.5 MILLION SAP USERS

2000 PROTECTED SAP SYSTEMS WORLDWIDE

200 SATISFIED CUSTOMERS

SAST

8 LANGUAGES
DE/EN/SP/FR/
CZ/RU/POR/CH

More languages comming

over 4000 automated SYSTEM CHECKS & SECURITY NOTES

3 times & SAP-certified
testified by Big 4 audit firm

Najlepsze praktyki bezpieczeństwa SAP – w momencie instalacji

SAP user

- Krytyczne autoryzacje
- Wyrafinowane matryce SOD
- User Master Record
- Standardowe Profile (SAP_ALL) oraz nieaktywni użytkownicy

ponad 600 ryzyk

Aplikacje

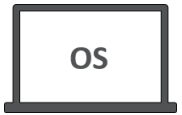
- Krytyczne ustawienia systemu
- Parametry systemu
- Konfigurowalne środki kontroli
- ABAP Workbench oraz Transport Management

ponad 3000 ryzyk

Bazy danych

- SAP DB oraz HANA
- Oracle
- IBM DB2
- Microsoft SQL-Sever

ponad 50 ryzyk



Operating System

- UNIX system checks
- Windows system checks
- AS400 system checks

ponad 50 ryzyk

SAST GRC SUITE - fakty

kompleksowość

- SAP **Security oraz GRC** dla Twojego systemu
- OS/net/DB
- Aplikacje i transakcje

integracja

- 100% ABAP
- **Instalacja jako add-on (import transportów)**
- Integracja z funkcjami SAP
- Centralna instalacja jeśli jest taka potrzeba

wiedza

- Używane w największych instalacjach SAP na świecie
- **Certyfikat SAP - NetWeaver, HANA oraz S/4HANA**
- Authorization checks oraz matryca SoD zweryfikowana przez Big4

ekonomia

- Praca produkcyjna w kilka godzin
- **Brak konieczności instalacji dodatkowego hardware/software**
- Szybka i intuicyjna praca operacyjna

Zarządzanie ryzykiem SAP

- Konflikty uprawnień – zarządzanie dostępami, mitygacja, kontrola, kompensacja
- Workflow zarządzania autoryzacjami
- Dostępy uprzywilejowane
- Podatności i weryfikacja ryzyk technicznych
- Pobieranie danych
- Monitorowanie SAP w SIEM

PYTANIA?
CHĘTNIE ODPOWIEM

Tomasz Jurgielewicz
Head of SAP Security

Tel: +48 508 400 203
Email: tomasz.jurgielewicz@lukardi.com
Web: https://lukardi.com/sap-data-security/