THE BLIND SPOT WITHIN THE SAP USER MANAGEMENT

13. March 2019, Bonn
PRIVILEGED ACCOUNTS - “KEYS TO THE IT KINGDOM”

EXTERNAL ATTACKERS

PRIVILEGED ACCESS
“Keys to the IT Kingdom”

MALICIOUS INSIDERS

Provides Proactive Protection and Detection
#1 Leader in Privileged Access Security

More than 4,400 customer globally

**FORTUNE**

Securing Privilege at more than 50% of the Fortune 500
CYBERARK PRIVILEGED ACCESS SECURITY SOLUTION

ENDPOINT PRIVILEGE MANAGER

Least Privilege and Credential Theft Protection for Workstations

CORE PRIVILEGED ACCESS SECURITY

Risk-based Credential Security and Session Management to Protect Against Attacks

ADVANCED

Least Privilege Server Protection | Domain Controller Protection

APPLICATION ACCESS MANAGER

Secrets Management for Applications, Tools, Containers and DevOps

ON-PREMISES HYBRID CLOUD
CyberArk positioned highest for ability to execute and furthest for completeness of vision
CYBERARK NAMED A LEADER IN PRIVILEGED IDENTITY MANAGEMENT

CyberArk ranks highest in current offering and market presence

Source: Forrester Research, Inc. Unauthorized reproduction, citation or distribution prohibited.
CROWN JEWELS
Sensitive Infrastructure, Assets, and Data

- DevOps
- Cloud Security
- IIOT / OT Security
- Identity Security
- Data Security
- SIEM and Threat Intelligence
- Network Security
- Endpoint Security
- Network Security
SECURING ERP & CRM SYSTEMS
CYBERARK BREAKS THE ATTACK CHAIN

Existing Access

On-Premises

Hybrid

Cloud

External Compromise

Internal Threats

External Threats

ESCALATE PRIVILEGES

Move Laterally

Perform Reconnaissance

Disrupt Business

Extract Data
NEW TARGETS – NEW THREATS?

According to VP Distinguished Analyst, Neil MacDonald

“As financially motivated attackers turn their attention ‘up the stack’ to the application layer, business applications such as ERP, CRM and human resources are attractive targets. In many organizations, the ERP application is maintained by a completely separate team and security has not been a high priority. As a result, systems are often left unpatched for years in the name of operational availability.”

Gartner, Hype Cycle for Application Security, 2017, July 2017

NEW THREATS?

• Hackers exploit vulnerabilities (multitude of ERP systems, versions, applications makes it easy)

• ERP applications touch more than just other ERP applications; infrastructure, operating systems, cloud consoles, etc.

• Very complex to begin with; also 4,000+ security patches making it nearly impossible to keep up*

*ERP Applications Under Fire: How cyberattackers target the crown jewels. Digital Shadows & Onapsis, July 2018
PRIVILEGED ACCOUNTS ACROSS THE MODERN IT STACK

- **Cloud Platform**
- **Operating System (IaaS)**
- **Backend Systems (IaaS, PaaS)**
- **Application Logic** (IaaS, PaaS, SaaS)
- **Databases**
- **Application Servers**
- **Cloud Platform**
- **Virtualization Layer**
- **Hardware**

Types of accounts:
- **e.g.** sap*, system, …
- **e.g.** sys, Service Accounts, …
- **e.g.** Administrator, root, …, ADM-John
- **e.g.** Cloud Management Consoles, Consoles of Virtualization Solutions
CHALLENGES IN SECURING SAP

• Main use cases are ERP software (e.g. S/4HANA), operational database system
• Provide security-specific features for their own applications
• SAP applications often owned by separate team; left unpatched for operational availability
• **Problem:** SAP applications touch all aspects of business, not just SAP-specific
Discover and onboard SAP privileged accounts via native CyberArk REST API.

DISCOVER ALL PRIVILEGED ACCOUNTS

SHORTEN THE TIME TO ONBOARD SAP SYSTEMS

CONNECT TO MULTIPLE SAP SYSTEMS

PACKAGE & ONBOARD ACCOUNTS DIRECTLY INTO CYBERARK
CYBERARK SOLUTIONS ENFORCE SAP BEST PRACTICES

BASED ON THE SECURE CONFIGURATION OF SAP NETWEAVER® APPLICATION SERVER USING ABAP

PROTECT SAP USERS
• Default users with default passwords
• SAP, DDIC, EARLYWATCH, SAPCPIC, and TMSADM

MANAGE SAP PRIVILEGED ACCOUNTS
• Dialog, system, communication, service and reference
• Java administrator in dual stack system

COMMUNICATE VIA SECURE NETWORK COMMUNICATION (SNC)
• SNC encrypts all traffic to SAP systems
• All communication from CyberArk to SAP via SNC

SECURE ACCESS TO SAP GUI
• Securing, isolating and monitoring privileged access through the SAP GUI
SECURING SAP UPGRADE PROCESS

- Upgrading SAP environments is a critical process, which can occur hundreds of times annually.
- The upgrade process affects production.
- Utilizing privileged access security capabilities to streamline upgrading via Software Update Manager (SUM).

PROTECTING THE SAP ENVIRONMENT

- Copying upgrade package
- Activate SUM
- Upgrade web app
- Check in
- Automatic rotated
SECURING ROBOTIC PROCESS AUTOMATION (RPA)
SECURING ROBOTIC CREDENTIALS IS PARAMOUNT

- RPA applications in your environment are a potential vulnerability management problem.
- Credentials used by bots provide an inherent risk within RPA when unmanaged and unprotected.
- Robots present one of the biggest consumers for credential security management!
START SECUREING BUSINESS CRITICAL APPLICATIONS & BOTS!
Thank you
www.cyberark.com