Managed Security Service
Current Threats in Cloud environments

Uemit Oezdurmus, 2020
Disclaimer

The information in this presentation is confidential and proprietary to SAP and may not be disclosed without the permission of SAP. Except for your obligation to protect confidential information, this presentation is not subject to your license agreement or any other service or subscription agreement with SAP. SAP has no obligation to pursue any course of business outlined in this presentation or any related document, or to develop or release any functionality mentioned therein.

This presentation, or any related document and SAP’s strategy and possible future developments, products and or platforms directions and functionality are all subject to change and may be changed by SAP at any time for any reason without notice. The information in this presentation is not a commitment, promise or legal obligation to deliver any material, code or functionality. This presentation is provided without a warranty of any kind, either express or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement. This presentation is for informational purposes and may not be incorporated into a contract. SAP assumes no responsibility for errors or omissions in this presentation, except if such damages were caused by SAP’s intentional or gross negligence.

All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, which speak only as of their dates, and they should not be relied upon in making purchasing decisions.
Motivation

Why do our customers need Security Services?
Common Security Breaches

Equifax Hack – 2017

An example that SAP Notes should used immediately. The security gap what is used here, was known months ago before the hack took place:

- **Massive data breach,**
- Equifax has confirmed that attackers entered its system in mid-May through a web-application vulnerability that had a patch available in March.
- Exposed personal data (social security numbers and addresses) of 143 million due to not applying any patches

Source: [https://www.wired.com/story/equifax-breach-no-excuse/](https://www.wired.com/story/equifax-breach-no-excuse/)

10KBLAZE / Potential SAP hacks 2019

“50,000 companies exposed to hacks of 'business critical' SAP systems: researchers” (Reuters)

- New ways to exploit vulnerabilities of systems that haven’t been properly protected
- If a company's security settings are not configured correctly, he said, a hacker can trick an application into thinking they are another SAP product and gain full access without the need for any login credentials.

Our Cloud Application Services Solution

Just Do It!

Perform Security Note Patching!

ca. 70% of all systems with critical and very critical status

Source: https://launchpad.support.sap.com/ewaworkspace
## Framework for HEC for Security

### Business Process Management
- Business Context

### Application Management
- Applications
- Middleware / Platform

### System Management
- System
- Database
- Operating System
- Virtualization

### IT Infrastructure Management
- Servers
- Storage
- Networking

<table>
<thead>
<tr>
<th>Business Process Management</th>
<th>Application Management</th>
<th>System Management</th>
<th>IT Infrastructure Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Context</td>
<td>Applications</td>
<td>System</td>
<td>Servers</td>
</tr>
<tr>
<td></td>
<td>Middleware / Platform</td>
<td>Database</td>
<td>Storage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Operating System</td>
<td>Networking</td>
</tr>
</tbody>
</table>

Legend:
- Blue: Completely managed by customer
- Green: Completely managed by service provider

<table>
<thead>
<tr>
<th>On Premise</th>
<th>IaaS</th>
<th>PM-CaaS</th>
<th>SaaS-like</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© 2020 SAP SE or an SAP affiliate company. All rights reserved.
Managed Security Services Portfolio

GDPR
- EU-GDPR Support Service
- Support Analysis
- Read Access Logging
- Field-Masking
- Blocking and Deletion with ILM
- User Interface Logging

Business Governance
- Managed Security Services for International Trade Management

Security for Cloud Products
- Managed Security Services for Success Factors

Platform Security
- Secure Cloud Connector
- End-to-End User Management
- Compliance Check in SCP

HEC
- Security Baseline Packages
- Security Risk Assessment
- Support Authorization Concept
- Security Starter Kit
- Security Monitoring
- Check & Apply SAP Security Notes

Compliance Check
- Audit Readiness Check
- Security Audit Log Set-up
- Segregation of Duty Check

Secure Interfaces
- RFC Security
- SNC & Kerberos Authentication for SAP GUI

Secure Users & Authorizations
- Security Advisory
- Security Strategy Planning and Management
- User and Role Management
- Authorization Upgrade
- Adjust Authorization Concept to Fiori
- Automated Authorization Test

GRC Solutions
- SAP Access Control
- SAP Risk Management
- SAP Identity Access Governance
- SAP Process Controls
- SAP Audit Management

Security Solutions
- Managed Security Services for Enterprise Threat Detection
- Code Vulnerability Analysis
- Penetration Testing

Managed Security Services Portfolio

Three lines of Defense
- Note: Portfolio Offerings with stand alone services and outcome based packages.

© 2020 SAP SE or an SAP affiliate company. All rights reserved.

Note: Portfolio Offerings with stand alone services and outcome based packages.
Threat intelligence
Security Layers

Possible attack vectors
High level Architecture SCP/HEC

Most preferred attack vector / surface
High level Architecture Hana Cloud
Where is the easiest way for hackers?
Commonly used target: User Phishing

Different ways to approach a user by using his/her attention by:

- Pharming (redirection to a bogus website)
- Smishing (using SMS as phishing tool)
- Vishing (Using Phone as phishing tool)
- Session hijacking (steal and misuse of user’s security token)
- Whaling (business email compromise, targeting C-level)
- Cloning (using malicious Website)
- Domain spoofing (URL of Website looks real, but isn’t)

Aiming to hijack or steal user credential
Benachrichtigung über die Verlängerung der Security Lizenzen

CISCO <example@email.example.com>

Wir haben festgestellt, dass Sie Verträge mit abgelaufenen Ablaufterminen haben, die Ihre Auffälligkeit erhöhen. Dank der Verlängerung stehen Sie sicher, dass Ihr Unternehmen vor potenziellen und bestehenden Bedrohungen geschützt bleibt.

Benötigen Sie weitere Informationen zu Ihren Security Lizenzverträgen? Haben Sie Fragen an einen Experten für Vertragsverlängerungen?

Wenden Sie sich an Ihren Ansprechpartner.

Hier ist eine Liste der Verträge mit abgelaufenen Ablaufterminen:

<table>
<thead>
<tr>
<th>Ablaufdatum</th>
<th>Software</th>
<th>Vertragsnummer</th>
</tr>
</thead>
<tbody>
<tr>
<td>21/02/2020</td>
<td>Identity &amp; Access</td>
<td>202244945</td>
</tr>
</tbody>
</table>
2020 Actuals (source TrendMicro)

COVID-19-Related Threats in Q1 2020

- **907K** Total spam messages related to COVID-19
- **737** Detected malware related to COVID-19
- **48K** Hits on malicious URLs related to COVID-19
- **220x** Increase in spam from Feb to Mar 2020
- **260%** Increase in malicious URL hits from Feb to Mar 2020

**United States**
Top location for spam and malware detections, and users accessing malicious URLs

*Detection numbers are based on the coverage of our Smart Protection Network, which has limited global detection/collection period: January 1 to March 31 (2020).*

---

The Countries Targeted Most by Malicious Coronavirus Spam

Countries targeted by largest share of global malicious spam emails with 'coronavirus' in the subject*

<table>
<thead>
<tr>
<th>Country</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>United Kingdom</td>
<td>20.8%</td>
</tr>
<tr>
<td>France</td>
<td>11.5%</td>
</tr>
<tr>
<td>United States</td>
<td>8.2%</td>
</tr>
<tr>
<td>Italy</td>
<td>5.9%</td>
</tr>
<tr>
<td>Belgium</td>
<td>5.2%</td>
</tr>
<tr>
<td>Germany</td>
<td>5.1%</td>
</tr>
<tr>
<td>India</td>
<td>4.9%</td>
</tr>
<tr>
<td>Netherlands</td>
<td>3.5%</td>
</tr>
</tbody>
</table>

* January 1 to March 27, 2020.
Source: Trend Micro
Critical and hard to identify – Advanced Persistent Threat (Wikipedia)

An advanced persistent threat (APT) is a prolonged and targeted cyberattack in which an intruder gains access to a network and remains undetected for an period of time. The intention of an APT attack is usually to monitor network activity and steal data rather than to cause damage to the network or organization.

Targeting business related systems of any kind, mainly used for:

- Steal Data
- Manipulate Data
- Manipulate systems
- Open backdoors for other hackers
Ransomware is a type of malware from cryptovirology that threatens to publish the victim’s data or perpetually block access to it unless a ransom is paid. While some simple ransomware may lock the system in a way which is not difficult for a knowledgeable person to reverse, more advanced malware uses a technique called cryptoviral extortion, in which it encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them.

Targeting business related systems of any kind, mainly used for:

- Manipulate / encrypt Data
- Sabotage of systems DB systems
- Open backdoors for other hackers

Example: Wannacry
What can we do to protect?
What to consider and protect – The end user

According to an independent survey of End Users:

80% would open suspicious emails and documents within their company’s network and devices, because they believed that those environments are much more protected than their private ones.

To strengthen IT Security, the imperative is to educate and train the end user in parallel to setting up company security policies and guidelines.
What to consider and protect – end-to-end security

- Processing Servers
- Database Servers
- Network FW/Switches
- Gateways
- Email Servers / User accounts
- Wifi Routers
- User end devices
- Mobile devices
What to consider and protect – network zones, segmentation and monitoring

Zone 1: Highly secure
- Critical internal systems and DBs
- Monitoring

Zone 2: Secure/Internal
- Non-critical internal systems and DBs (e.g. Info panels)

Zone 3: Fenced/Internal DMZ
- Non-critical internal systems and DBs (e.g. Training)

Zone 4: Internet DMZ
- Internet systems (e.g. Marketplaces)

Zone 5: Public Internet
- Internet systems (e.g. Company Infos)

Monitoring with SIEM solutions

With SAP Enterprise Threat Detection on suspicious activities
Managed Security Services Portfolio

GDPR
- EU-GDPR Support Service
- Technical Analysis
- Read Access Logging
- Field-Masking
- Blocking and Deletion with ILM
- User Interface Logging

Business Governance
- Managed Security Services for International Trade Management

SCP (Add-on)
- Secure Cloud Connector
- End-to-End User Management
- Compliance Check in SCP

Security for Cloud Products
- Managed Security Services for Success Factors

Platform Security
- HEC
- On-Premises

HEC
- Security Baseline Packages
- Security Risk Assessment
- Support Authorization Concept
- Security Starter Kit
- Security Monitoring
- Check & Apply SAP Security Notes
- Compliance Check
- Audit Readiness Check
- Security Audit Log Set-up
- Segregation of Duty Check
- Secure Interfaces
- RFC Security
- SNC & Kerberos Authentication for SAP GUI
- Secure Users & Authorizations
- Security Advisory
- Security Strategy Planning and Management
- User and Role Management
- Authorization Upgrade
- Adjust Authorization Concept to Fiori
- Automated Authorization Test

GRC Solutions
- SAP Access Control
- SAP Risk Management
- SAP Identity Access Governance
- SAP Process Controls
- SAP Audit Management

Security Solutions
- Managed Security Services for Enterprise Threat Detection
- Code Vulnerability Analysis
- Penetration Testing

Note: Portfolio Offerings with stand alone services and outcome based packages.

Infrastructure Security
- HANA Security
- Infrastructure Security Assessment

© 2020 SAP SE or an SAP affiliate company. All rights reserved.
Q & A
Thank you.

Contact information:

Uemit Oezdurmus
Global Head Managed Security Services
SAP Deutschland SE & Co.KG
T +49 175-2773725
E uemit.oezdurmus@sap.com