

SAP Application Security

Your Crown Jewels Online: Further Attacks to SAP Web Applications

Mariano Nunez
CEO – Onapsis, Inc.



Session ID: HT2-301

Session Classification: Lightning Round

RSACONFERENCE2012

Agenda

- The evolution of the threats to SAP systems
- The different SAP Web Servers
- Attacks to SAP Web Applications
 - Attacks to the SAP Web Dispatcher
 - Live demo: Business data exfiltration
 - Live demo: Authentication bypass in Enterprise Portals
- Countermeasures

The evolution of the threats to SAP systems



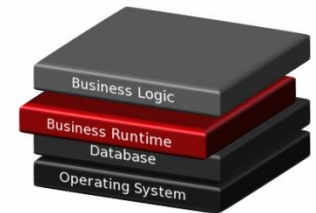
What is SAP?

- Largest provider of business management solutions in the world.
- Used by Fortune-500 world-wide companies, governmental organizations and defense facilities to **run their every-day business-critical processes.**



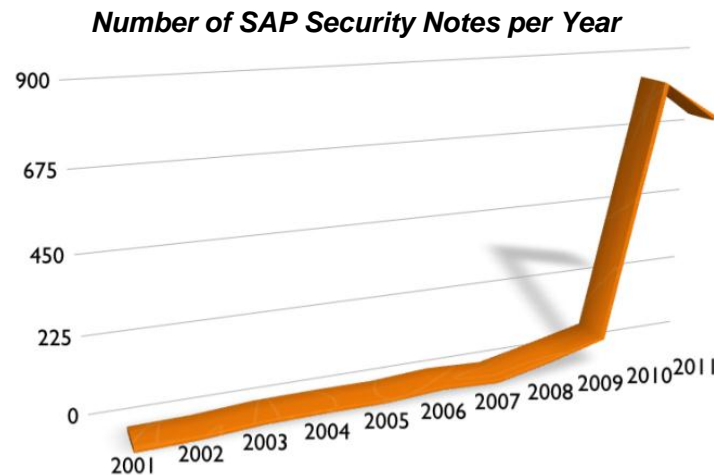
What does “SAP Security” means?

- SAP Security was traditionally regarded as a synonym of “Segregation of Duties controls”.
- But... **SoD controls are not enough!**
- The forgotten layer: The Business Infrastructure (NetWeaver/Basis).
 - Base framework in charge of critical tasks such as authentication, authorization, auditing, logging, etc
 - Can be susceptible of security vulnerabilities that, if exploited, can lead to **espionage, sabotage and fraud** attacks to the business information.



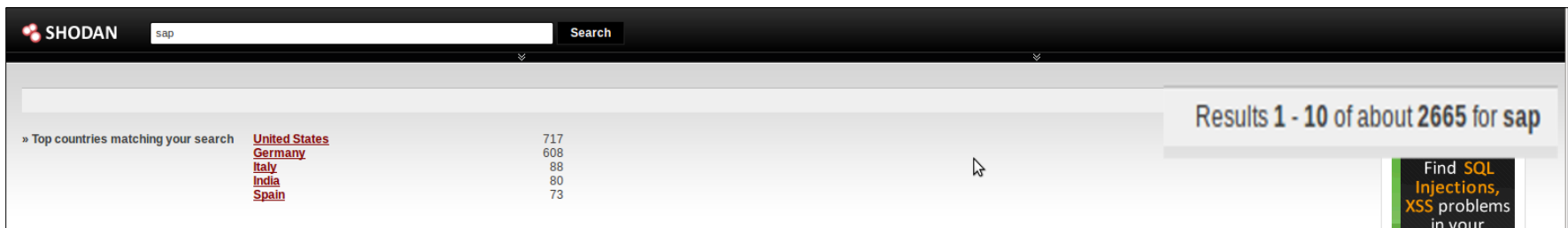
Attacks to the SAP technical layer

- Involves much higher risks than SoD violations:
In many cases, the attacker does not even need a user account in the system!
 - i.e.: By default, a remote attacker can take complete control of SAP Application Servers anonymously by exploiting vulnerabilities in the SAP Gateway.



“My SAP system is only used internally”

- Could be true a decade ago, probably not anymore.
- Attackers can easily find SAP systems online.



SHODAN search results for 'sap'. The search bar shows 'sap' and the results are 'Results 1 - 10 of about 2665 for sap'. A table lists top countries matching the search:

Country	Count
United States	717
Germany	608
Italy	88
India	80
Spain	73

Find SQL Injections, XSS problems in your



inurl:/irj/portal



Search

Page 19 of 187 results (0.15 seconds)

Advanced search

The different SAP Web Application Servers



SAP Web Application Servers

- **SAP Internet Transaction Server (ITS)**
 - Released in 1996.
 - Middleware that translates SAP screens to HTML.
- **SAP Web Application Server (WebAS)**
 - The SAP kernel was enhanced to support HTTP(S).
 - Access provided by *ICF services*.
- **SAP Enterprise Portal (EP)**
 - Based in the SAP J2EE Engine.
 - Unique point of Web access to SAP systems.

The SAP Web Dispatcher

- Reverse-proxy mainly used for balancing the load to backend SAP Web servers.
- Based on the ICM framework.
- Features a Web Administration Interface.

If the SAP Web Dispatcher is exploited, all the backend systems can be ultimately compromised.

Attacks to SAP Web Applications



Attacks to the SAP Web Dispatcher

- It is possible to identify whether a Web Dispatcher is present by:
 - Analyzing returned HTTP headers
 - Sending specially-crafted requests that trigger error conditions.
 - Trying to access the Administration interface.
- Once compromised, an attacker may increase the *trace level* and obtain valid credentials/cookies to access the backend systems.

Attacks to the SAP Web Dispatcher

The screenshot displays the SAP Web Administration Interface (Web Administration Interface) for the SAP Web Dispatcher. The browser address bar shows the URL: labsaprv017:8030/sap/wdisp/admin/public/default.html. The interface is divided into a left-hand navigation menu and a main content area displaying system logs.

SAP Web Administration Interface

SAP Web Dispatcher Menu (labsaprv017_30)

- Core System
 - Monitor
 - Active Services
 - Core Thread Status
 - Active Connections
 - Trace
 - Parameters
 - Hostname Buffer
 - Release Information
 - Statistic
 - MPI Status
 - ICM Security Log
- HTTP Handler
 - Access Log
 - Server Cache
 - Access Handler
 - Admin Handler
 - Modification Handler
- Dispatching Module
 - SSL End To End Dispatching
 - URL Filter
 - Parameters

System Log Output:

```
request_buf_used: 0 response_buf_used: 0
request_buf_offset: 0 response_buf_offset: 0

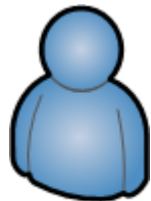
[Thr 139684408948496] IcmReadFromConn(id=2/8): request new MPI (0/0)
[Thr 139684408948496] IcmLowOnBlocks: mpi buffer space free (cur/limit/unreserved): 0/179/224)
[Thr 139684408948496] MPI<b2>b#23 GetOutbuf 0 20dle8 65536 (0) -> 7f0ad5229208 5242880 MPI_OK
[Thr 139684408948496] NiIRead: hdl 81 received data (rcd=676,pac=1,RAW_IO)
[Thr 139684408948496] NiIRead: hdl 81 recv would block (errno=EAGAIN)
[Thr 139684408948496] NiIRead: raw read for hdl 81 timed out (0ms)
[Thr 139684408948496] IcmReadFromConn(id=2/8): read 676 bytes, 1 readops (timeout 0)
[Thr 139684408948496] Address Offset IcmReadFromConn received
[Thr 139684408948496] -----
[Thr 139684408948496] 7f0ad5229250 000000 47455420 2f736170 2f62632f 6775692f |GET /sap/bc/gui/|
[Thr 139684408948496] 7f0ad5229260 000016 7361702f 6974732f 77656267 75693f73 |sap/its/webgui?s|
[Thr 139684408948496] 7f0ad5229270 000032 61702d73 79737465 6d2d6c6f 67696e2d |ap-system-login-|
[Thr 139684408948496] 7f0ad5229280 000048 62617369 635f6175 74683d58 26736170 |basic_auth=X&sap|
[Thr 139684408948496] 7f0ad5229290 000064 2d636c69 656e743d 32303026 7361702d |-client=200&sap-|
[Thr 139684408948496] 7f0ad52292a0 000080 6c616e67 75616765 3d454e20 48545450 |language=EN HTTP|
[Thr 139684408948496] 7f0ad52292b0 000096 2f312e31 0d0a486f 73743a20 6c616273 |/1.1..Host: labs|
[Thr 139684408948496] 7f0ad52292c0 000112 61707372 76303137 3a383033 300d0a43 |apsrv017:8030..C|
[Thr 139684408948496] 7f0ad52292d0 000128 6f6e6e65 6374696f 6e3a206b 6565702d |onnection: keep-|
[Thr 139684408948496] 7f0ad52292e0 000144 616c6976 650d0a43 61636865 2d436f6e |alive..Cache-Con|
[Thr 139684408948496] 7f0ad52292f0 000160 74726f6c 3a206d61 782d6167 653d300d |trol: max-age=0.|
[Thr 139684408948496] 7f0ad5229300 000176 0a417574 686f7269 7a617469 6f6e3a20 |.Authorization: |
[Thr 139684408948496] 7f0ad5229310 000192 42617369 6320576b 394f5156 42545356 |Basic Wk90QVBTSV|
[Thr 139684408948496] 7f0ad5229320 000208 4d365432 35686348 4e70637a 45794d77 |M6T25hcHNpczEyMw|
[Thr 139684408948496] 7f0ad5229330 000224 3d3d0d0a 55736572 2d416765 6e743a20 |==..User-Agent: |
[Thr 139684408948496] 7f0ad5229340 000240 4d6f7a69 6c6c612f 352e3020 28583131 |Mozilla/5.0 (X11|
[Thr 139684408948496] 7f0ad5229350 000256 3b204c69 6e757820 7838365f 36342920 |; Linux x86_64) |
[Thr 139684408948496] 7f0ad5229360 000272 4170706c 65576562 4b69742f 3533352e |AppleWebKit/535.|
```

Attacks to the SAP Web Application Server - *Exploitation of RFC over the Internet*

- RFC is a proprietary protocol widely used by SAP. We presented threats and attack vectors in BlackHat 2007.
- This interface is (usually) only accessible internally.
- But... there is an ICF Service that can be used to perform RFC calls.

If this service is enabled, a remote attacker can perform RFC calls to the SAP Web Application Server, just as he was sitting in the local network!

Attacks to the SOAP RFC Service



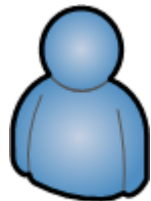
User



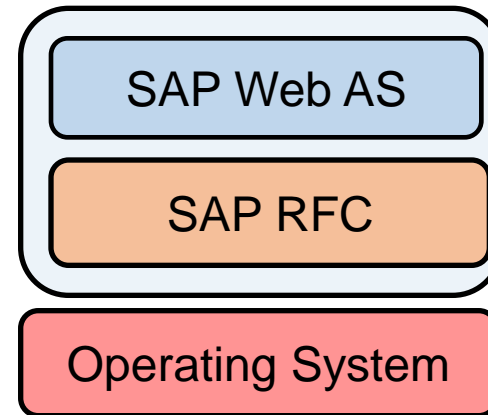
SAP Web
Application Server



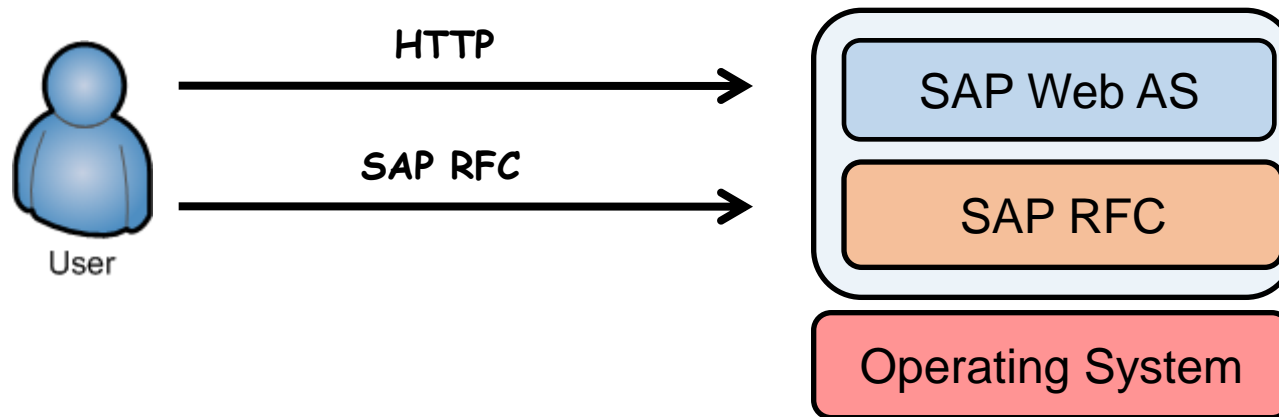
Attacks to the SOAP RFC Service



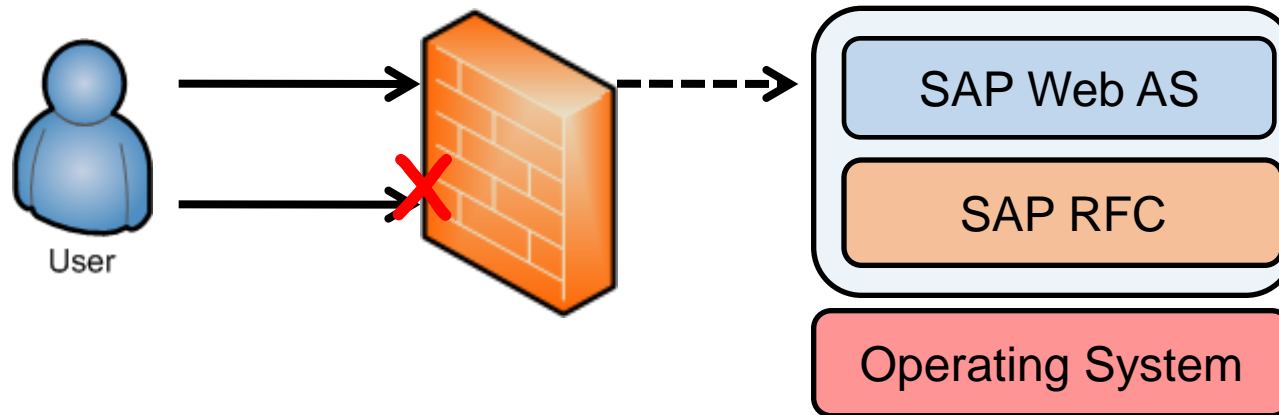
User



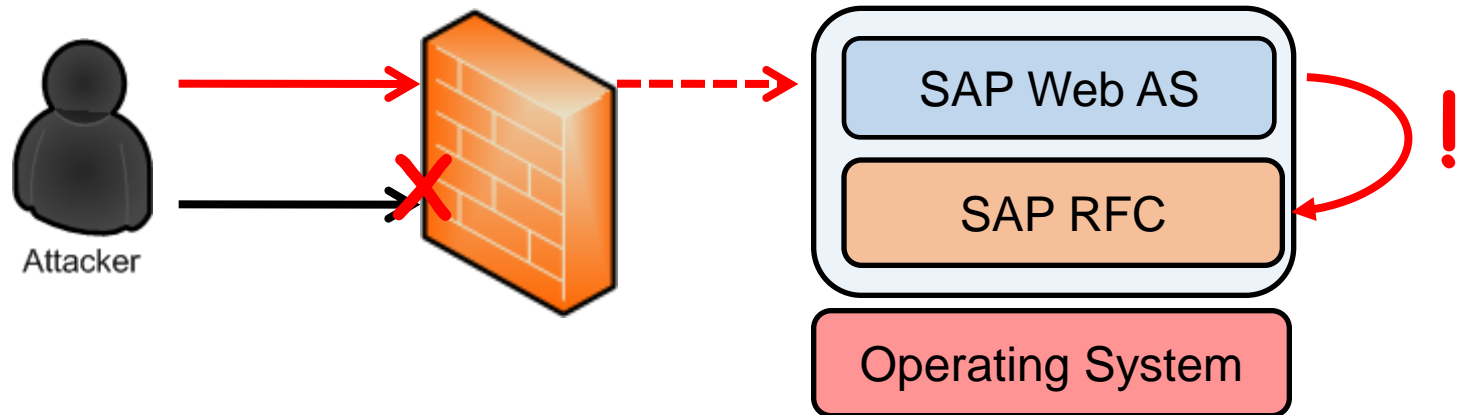
Attacks to the SOAP RFC Service



Attacks to the SOAP RFC Service



Attacks to the SOAP RFC Service



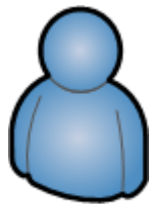
Live Demo: Business data exfiltration attacks through the Web



Authentication Bypass Attacks

- Many organizations currently have Web Access Management (WAM) solutions in place.
- They use them to enable secured access to the systems (tokens, biometrics, etc) and Single-Sign On.
 - RSA ClearTrust
 - CA SiteMinder
 - Oracle Oblix
 - Entrust GetAccess
 - Microsoft Integrated Windows Authentication
- The SAP J2EE Engine integrates with them using the *Header Variable Login Module...*

The Header Authentication Scheme



User



Firewall



Authentication Proxy



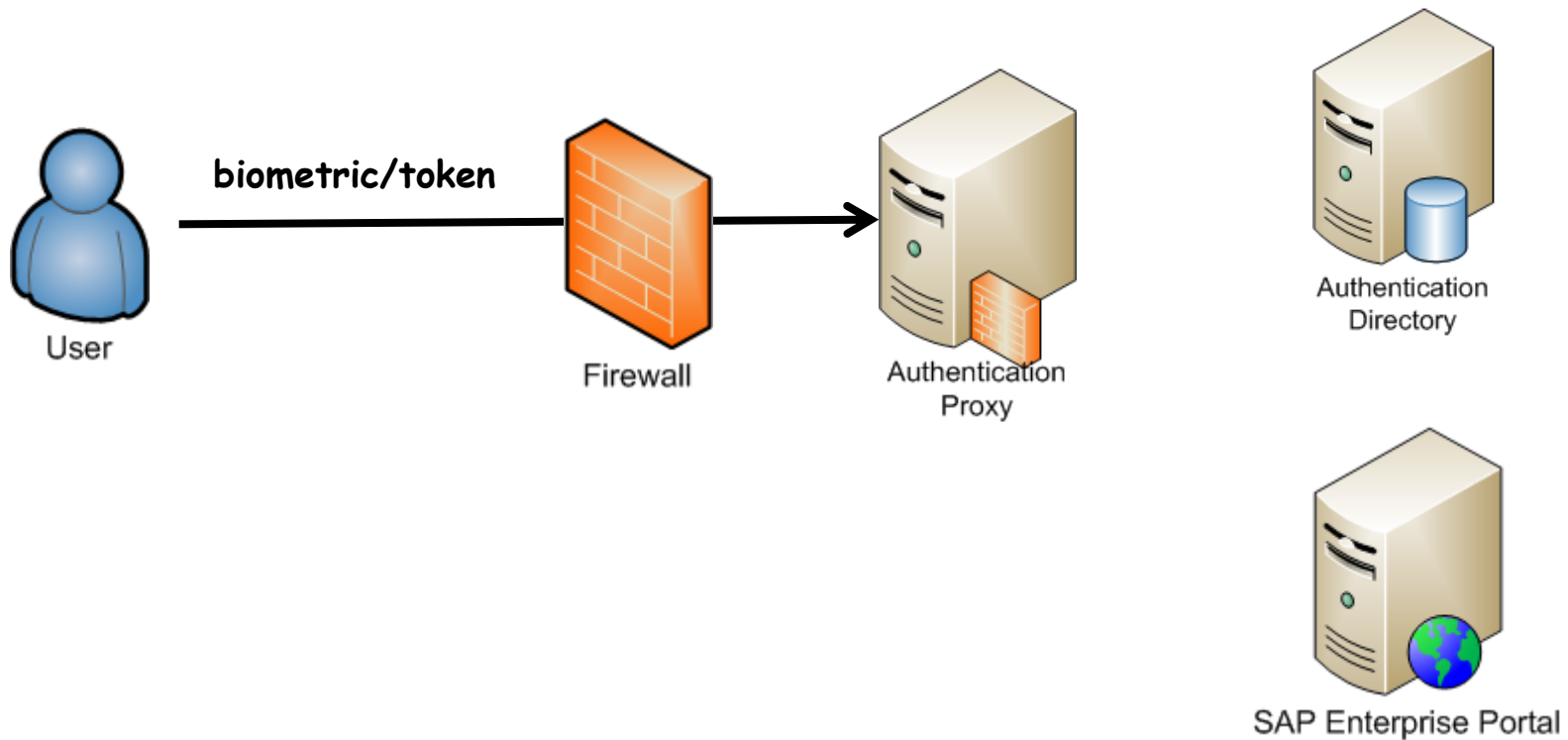
Authentication Directory



SAP Enterprise Portal

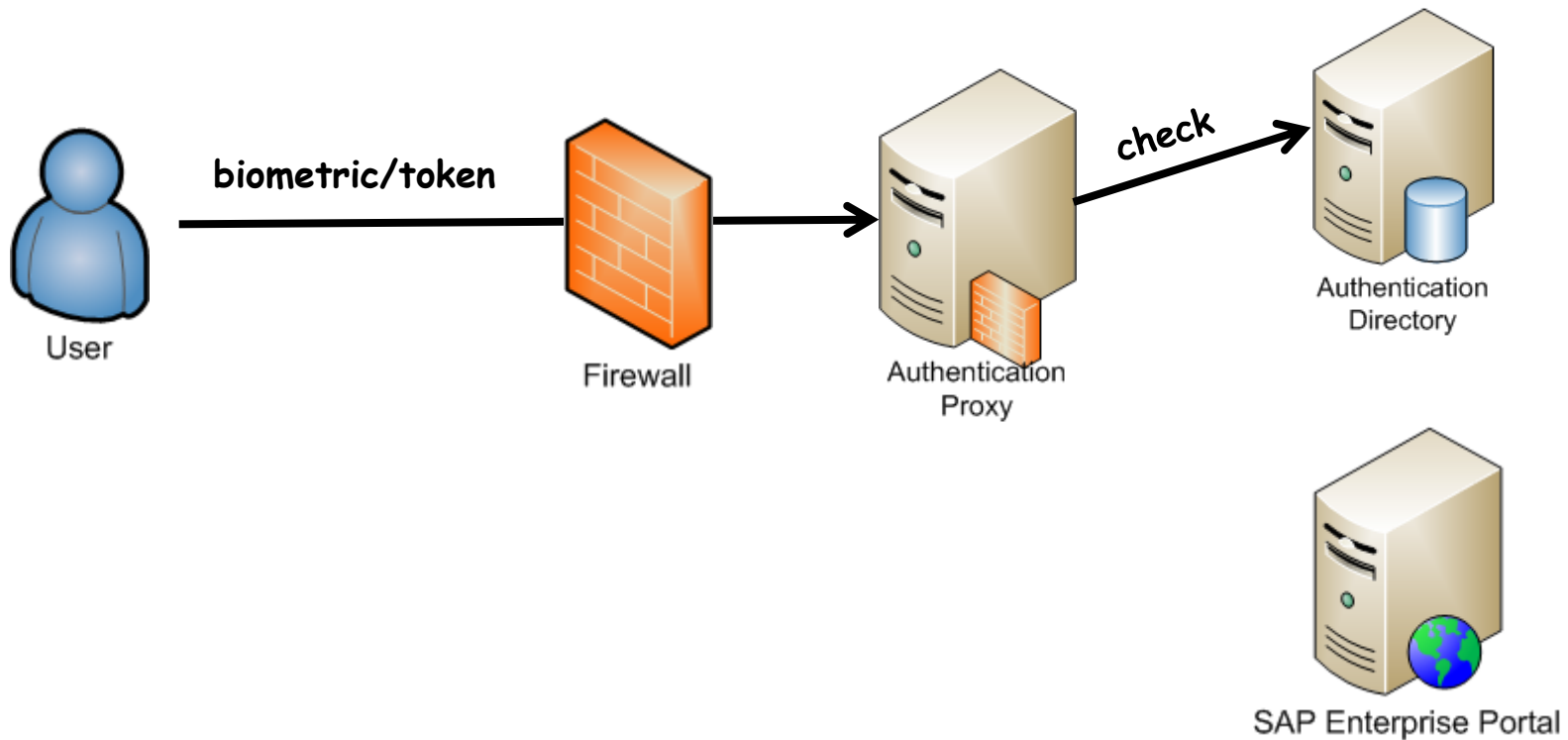


The Header Authentication Scheme



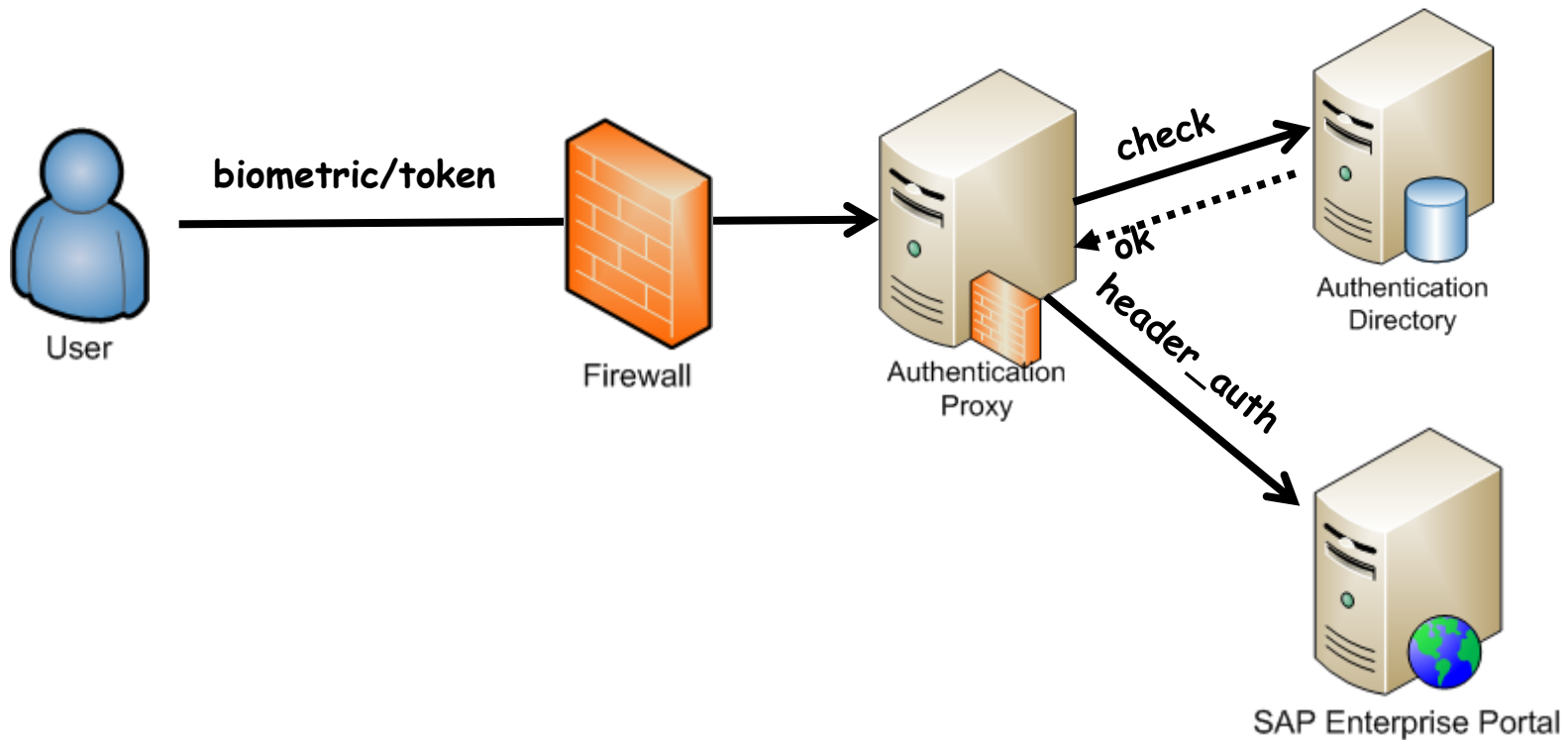
1. The user provides authentication information to the EAM/WAM solution.

The Header Authentication Scheme



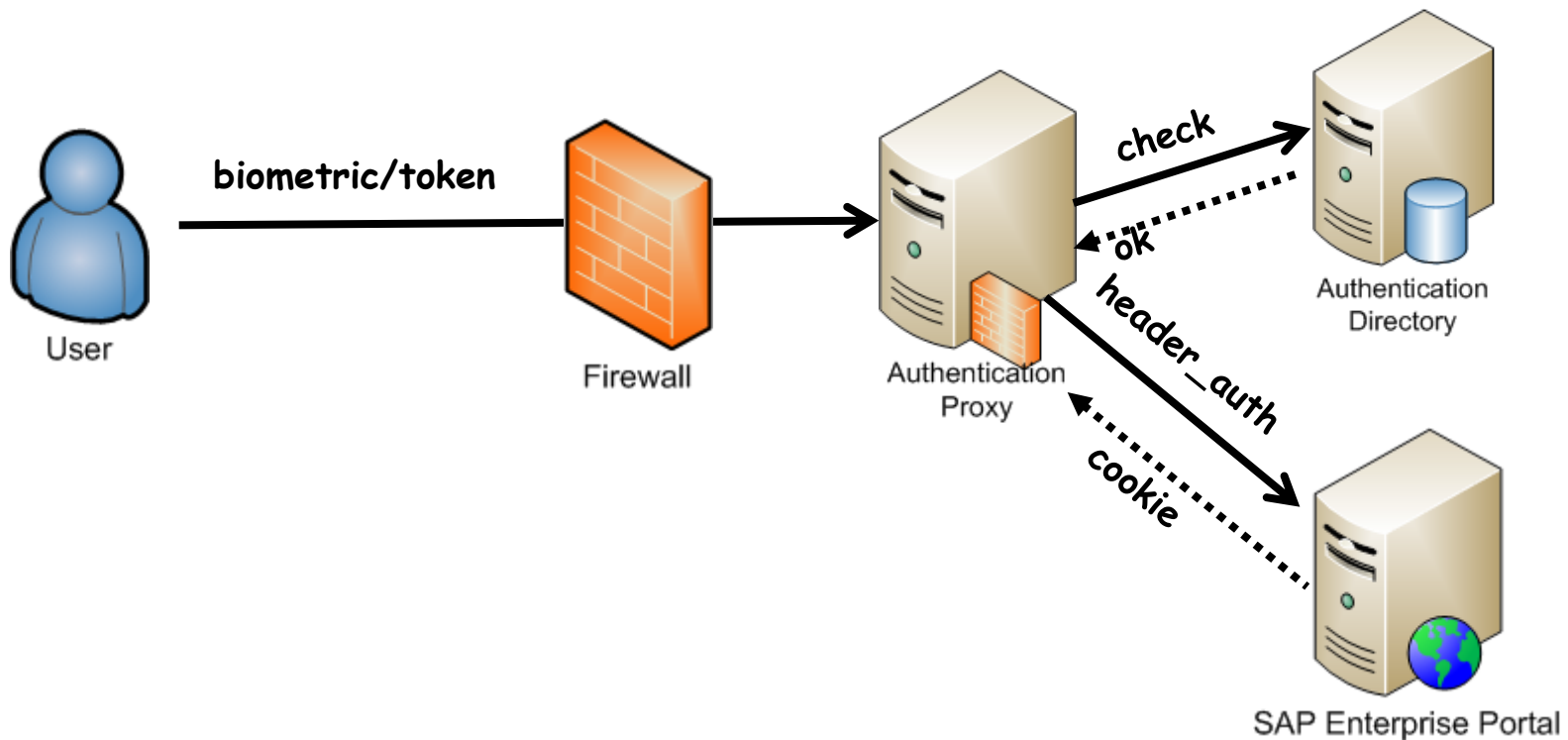
2. The solution checks provided credentials.

The Header Authentication Scheme



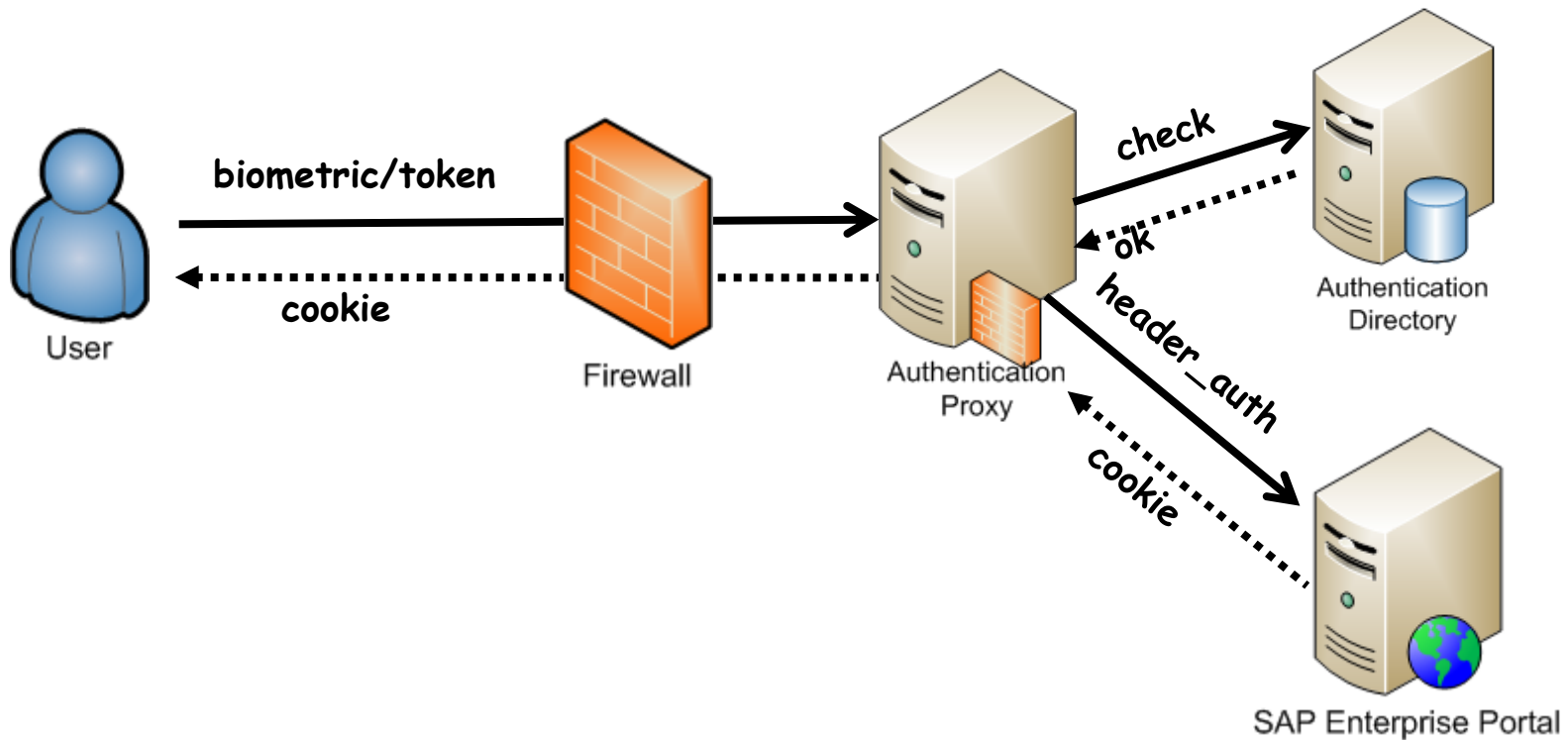
3. If successful, connects to the Enterprise Portal and sends the user to authenticate in a HTTP header.

The Header Authentication Scheme



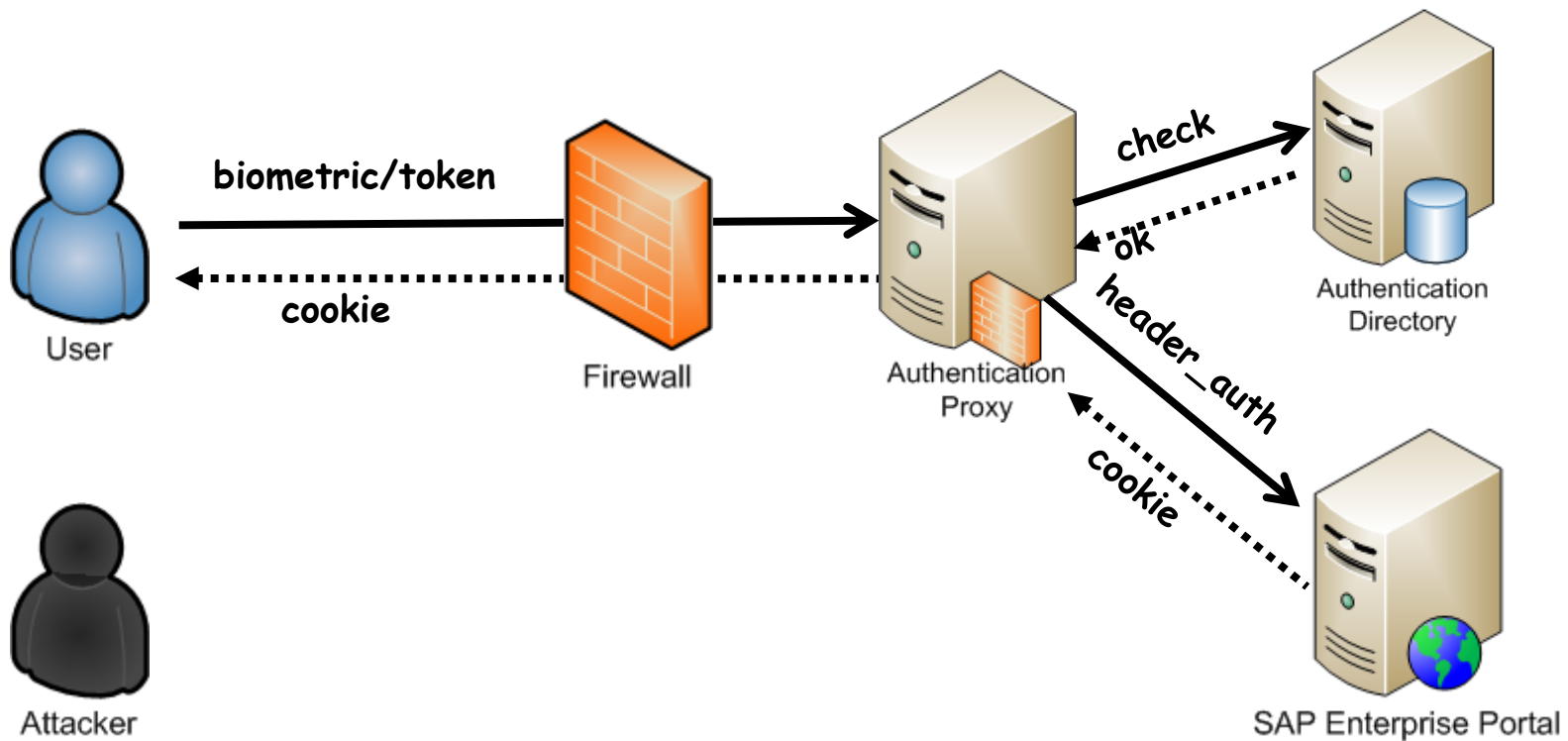
4. The Enterprise Portal verifies that the user is valid (it exists), and returns an SAP SSO logon ticket to the user.

The Header Authentication Scheme



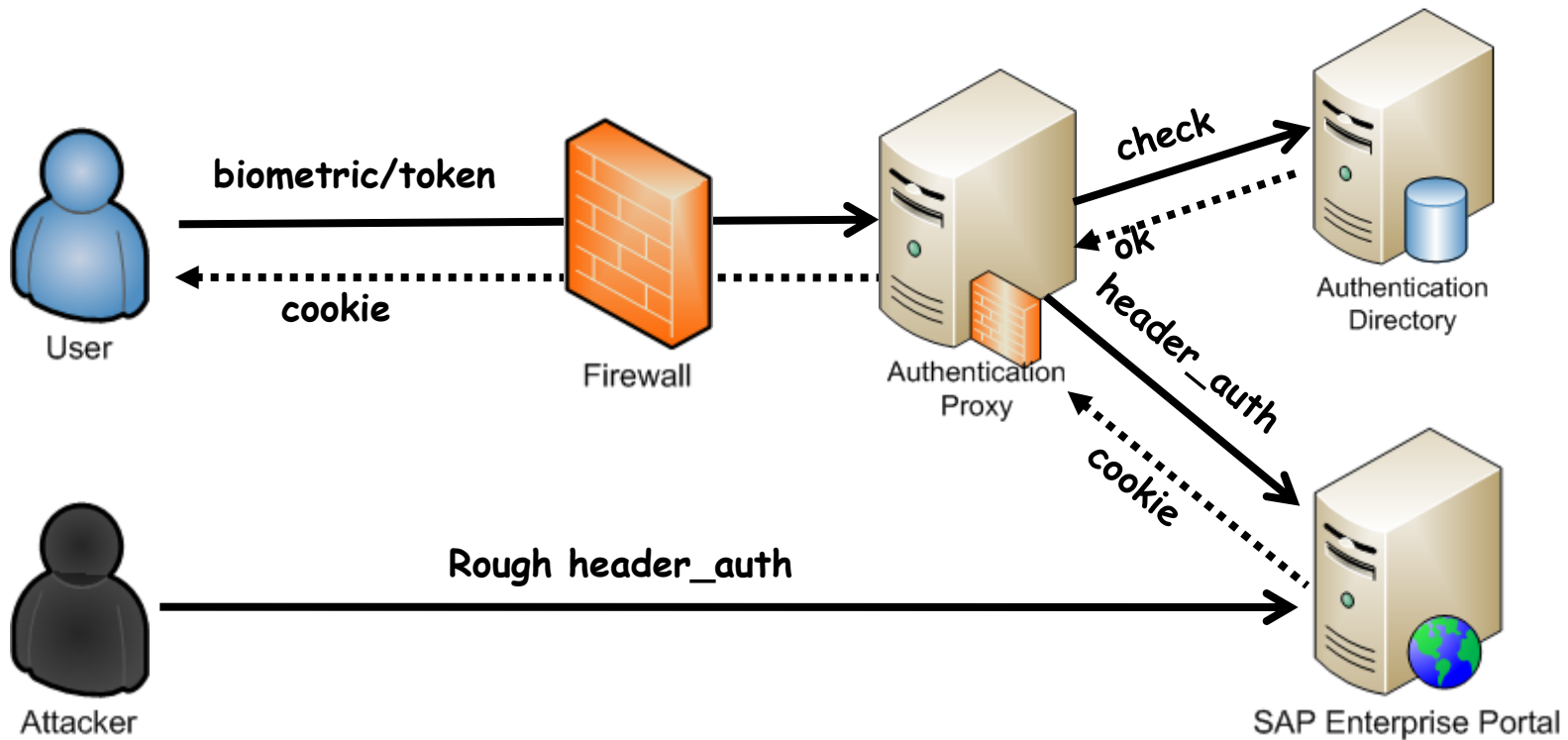
5. The user is authenticated.

The Attack



If the attacker can connect directly with the SAP Enterprise Portal, nothing prevents him from impersonating the EAM/WAM solution!

The Attack



If the attacker can connect directly with the SAP Enterprise Portal, nothing prevents him from impersonating the EAM/WAM solution!

Live Demo: Attacks to SAP Enterprise Portal Authentication



How to protect yourself from these attacks

■ Attacks to ICF Services:

- Disable any ICF service that is not enabled due to business requirements.
- Check SAP Note 1498575 and [1].
- Maintain ICF Authorization Data as described in [2] and [3].

■ Attacks to NetWeaver Portal authentication:

- Implement proper network filters to avoid direct connections to the SAP J2EE Engine.
- If using it for Windows authentication, switch to the SPNegoLoginModule.
- Check [4].

1. <http://www.sdn.sap.com/irj/scn/index?rid=/library/uuid/f0d2445f-509d-2d10-6fa7-9d3608950fee>
2. http://help.sap.com/saphelp_nw73ehp1/helpdata/en/39/e11482b2d23a428e583a59bef07515/frameset.htm
3. http://help.sap.com/saphelp_nw73ehp1/helpdata/en/9f/fc5e900b62d94e8878eb94db5b986f/frameset.htm
4. http://help.sap.com/saphelp_nw73ehp1/helpdata/en/d0/a3d940c2653126e10000000a1550b0/frameset.htm

Conclusions

- SAP systems are more and more connected to the Internet. Furthermore, few companies have internal DMZs for SAP servers.
- SAP Web Application Servers are highly complex and need to be fully understood to be able to secure them.
- By exploiting vulnerabilities in SAP Web components, an anonymous attacker can obtain complete control of the internal SAP servers and perform espionage, sabotage and fraud attacks.

Apply

- Find out which SAP Webapps you are using.
 - If not required, disable them.
 - If connected to the Internet, deploy WAF/IPS.
- Detect vulnerable Web services and configurations that could be exposing your business information and disable them.
- Evaluate ALL the systems (not just Production), at least after each SAP Security Patch Day.

