Compliance in the Cloud

PRESENTED BY:
Gary Newe, RVP, Systems Engineering
SWIFT Payment Network

• $60M transferred to hackers’ accounts
• Hacked the www. of the Polish Banking Authority
• Set up a Watering Hole
• Used these credentials to gain access to terminals in banks
• Moved sideways to SWIFT terminals
• Winner, winner…
• Until a TYPO spoiled their fun
Let’s Review

Compliance ≠ Security
There Is No Cloud...

SPECTRE

MELTDOWN

Row Hammer

Google cloud VMs given same IP addresses ... and down they went

Yikes! And the fix is to delete and rebuild the VM.

By Simon Sharwood, APAC Editor 17 Jun 2018 at 23:23

Google and Microsoft Reveal New Spectre Attack

Security researchers from Google and Microsoft have found two new variants of the Spectre attack that affects processors made by AMD, ARM, IBM, and Intel.
Cloud Top Threats

- Data Loss
- Insufficient Identity and Access Management
- Application and API Vulnerabilities
- Insufficient Due Diligence
- Shared Technology Vulnerabilities
- Denial of Service
Security Is Still on the Outside Looking In

- Rarely integrated into DevOps
- Needs to happen at EVERY stage of the DevOps lifecycle
  - Not just technology conversation
  - About people, processes, training
Security in the Cloud

- Cloud providers can significantly improve security… to a certain degree.
- Important to remember who owns data, risk, and compliance.
- On their own, CSP behaviour and tools will be insufficient to meet all GDPR compliance requirements.
- While Azure and AWS have tools to help you with compliance, they can’t make you compliant.
Risk Management

Avoid
Accept
Reduce
Share
Cloud can help organizations increase security posture.

Data and risk is always owned, never transferred.

AWS, Azure, and Google all have mature security programs and ISO certification, amongst many others.

---

Source: Shared Responsibilities for Cloud Computing, Microsoft, April 2017
GDPR vs The Rest

• Others tend to be prescriptive and check-box
  • Architecture, firewalls, encryption… even down to specific versions of TLS.
  • Compliance is (for the most part) not subjective.
  • Often considers only the technical controls.

• GDPR
  • Non-prescriptive, risk based.
  • Compliance may be subjective, much of the risk is proof of risk/privacy assessments and what you’ve done to minimise impact.
  • Technical, people, process.
GDPR

**Personal Privacy**
- Personal data
- Accurate
- Up to date
- Right to erasure
- Opt in and out
- Control over its use

**Safe and Secure**
- Confidentiality
- Integrity
- Availability
- Resilience
- *State of the art vs. risk-based*

**Transparency**
- Clear notification of collection
- Used only for intended purposes
- *Breach notifications* (72 hours to DPA)

**IT and Contracts**
- Internal training
- Document and audit policies
- Employ DPO (if applicable)
- Create and manage compliant vendor contracts
### GDPR Territorial Scope

- Offers or directs services (free or paid) to a subject in the EU
- Monitors activities of a subject who is a member of the EU

<table>
<thead>
<tr>
<th>Party has establishment in EU Article 3 (1)</th>
<th>Party offers goods or services to, or monitors persons, resident in EU</th>
<th>GDPR applies? Article 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Y</td>
<td>Y</td>
<td>YES</td>
</tr>
<tr>
<td>Y</td>
<td>N</td>
<td>YES</td>
</tr>
<tr>
<td>N</td>
<td>Y</td>
<td>YES ¹</td>
</tr>
<tr>
<td>N</td>
<td>N</td>
<td>NO</td>
</tr>
</tbody>
</table>

Party has establishment in EU Article 3 (1) Party offers goods or services to, or monitors persons, resident in EU GDPR applies? Article 3
GDPR Territorial Scope: Consumer in EU

CRM Cloud (Data Processor) → VDI → Consumer (Data Subject) → Support Staff (Data Controller) → Service Provider (Data Controller)
GDPR Territorial Scope: Party in EU

Consumer (Data Subject)

Service Provider (Data Controller)

Cloud Storage (Data Processor)
Who Must be Compliant?

Data Subject  
e.g. Consumer / Staff Member

Data Controller(s)  
e.g. Service Provider

Data Processor(s)  
e.g. Cloud

General Data Protection Regulation  
(EU) 2016/679

“The controller shall use only processors providing sufficient guarantees”  
– GDPR Article 28(1)
Security != Privacy

1. Apply database encryption
2. Use HTTPS
3. ???
4. Profit

Breach
Web app attacks are the #1 single source entry point of successful data breaches.
“Use CSP-provided tools where your risk assessment identifies that they can adequately address that part of the GDPR problem. However, third-party tools may be more effective, in particular when they can be used across CSPs.”

- Gartner
<table>
<thead>
<tr>
<th>OWASP Top 10 2017</th>
<th>Core Rule Set 3.0 Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1: Injection</td>
<td>![Thumb Down]</td>
</tr>
<tr>
<td>A2: Broken Authentication</td>
<td>![Thumb Down]</td>
</tr>
<tr>
<td>A3: Sensitive Data Exposure</td>
<td>![Thumb Down]</td>
</tr>
<tr>
<td>A4: XML External Entities (XEE)</td>
<td>![Thumb Up]</td>
</tr>
<tr>
<td>A5: Broken Access Control</td>
<td>![Thumb Down]</td>
</tr>
<tr>
<td>A6: Security Misconfiguration</td>
<td>![Thumb Down]</td>
</tr>
<tr>
<td>A7: Cross-Site Scripting (XSS)</td>
<td>![Thumb Up]</td>
</tr>
<tr>
<td>A8: Insecure Deserialization</td>
<td>![Thumb Up]</td>
</tr>
<tr>
<td>A9: Using Components with Known Vulnerabilities</td>
<td>![Thumb Down]</td>
</tr>
<tr>
<td>A:10 Insufficient Logging and Monitoring</td>
<td>![Thumb Down]</td>
</tr>
</tbody>
</table>
Some actually don’t deliver complete OWASP mitigation, even though it’s considered baseline functionality.

While some deliver regulatory compliance, that’s not an effective security strategy.

Blacklisting can defeat known bad requests, but what it doesn’t know can be used to bypass it.

Does not take into account evolving attack vectors.

(Layer 7 DDoS, Intellectual property theft, Bot attacks, etc.)
Advanced WAF

Traditional WAF
- OWASP Top 10
- Regulatory Compliance
- Blacklisting

Advanced WAF
- Proactive Bot Defence
- Credential Protection
- Mobile App Security
- DDoS Defence
- Client-Side Integrity Defence
- API Security
Principles

Article 5

- Fair, lawful, transparent
- Purpose limitation
- Data minimisation
- Accurate and up-to-date
- Retention limitation
- Safe and secure
1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

a) the pseudonymization and encryption of personal data;

b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.
Security of Processing

Article 32

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

   a) the pseudonymization and encryption of personal data;

   b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

   c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

   d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.
Confidentiality and Integrity

Solutions
Access Protection

GDPR CHALLENGE

Unauthorised access affecting **confidentiality and integrity** of data

- Malicious access attempts
- Least privilege violations
- User password fatigue
- Lack of endpoint visibility
- Phishing attacks
- Malware on client endpoints
- Bot disruption

SOLUTION

**Secure authentication**

- Multi-Factor Authentication (MFA)
- Federation
- SAML 2.0 / OAuth 2.0

**Granular and context-aware access**

**Single sign-on (SSO)**

**Endpoint detection and protection**

- Phishing detection
- Credential theft prevention
Unauthorised access affecting confidentiality and integrity of data

Context Is Key

- Authentication
- Device type and integrity
- Operating system
- Network integrity
- Browser
- Location
- Access method
- Network quality and availability
- App location
- App importance and risk
- App type / version
- Connection integrity
SOLUTION 1
Risk-based policy protection
SOLUTION 2

Credential protection

App-layer encryption

Goes beyond TLS/SSL

088373be1 = lsdkwe9
0x8xb28 = pei57

TLS

User = user
Password = 12345

F5 Advanced WAF

Field name obfuscation
Field value encryption

AJAX JSON Support

Stolen credentials are encrypted and cannot be re-used

No app updates required
SOLUTION 3

Federated identity for cloud access

Application Infrastructure

Corporate Users

Applications

Access Protection

MFA

VPN

Directory Services

SSO Context-Based Auth

Federation

Office 365
Google Apps
Salesforce
SaaS Providers

Users

Attackers

SAML 2.0
OAUTH 2.0
Application Protection

GDPR CHALLENGE

Cyber attacks on vulnerable web apps affect **confidentiality, integrity, and availability**.

- OWASP Top 10 threats
- Credential stuffing
- Malicious bots
- L7 DDoS attacks
- Session hijacking

SOLUTION

Advanced Web Application Firewall (WAF)

- Session tracking to identify bad actors
- Virtual patching to block attacks on vulnerable code
- Bot detection and prevention
- DAST integration
- Data cloaking
SOLUTION

Web application firewall, cloud, or on-premises
Availability and Resilience

Solutions
Security of Processing

Article 32

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

a) the pseudonymization and encryption of personal data;

b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.
Denial of Service Protection

**GDPR CHALLENGE**

*Availability of data affected by growing DDoS attacks*
- **Volumetric** – flood attacks on layers 3-4, 7
- **Asymmetric** – invoke timeouts or session-state changes
- **Computational** – consume CPU and memory
- **Vulnerability-based** – exploit application software vulnerabilities

**SOLUTION**

**DDoS protection**
- Layers 3-7 attack detection and prevention
- Upstream scrubbing service
- Mitigate multi-vector, burst attacks
SOLUTION

Multi-layered, application-aware DDoS mitigation
Increased Resilience

GDPR CHALLENGE

Single cloud provider risks lack of resilience.

- Cloud is another supply chain issue.
- Single DNS provider could take out entire organization.
- Catastrophic failure of cloud provider risks data loss.
- Are backup RPO and RTO sufficient for GDPR?

SOLUTION

Multi-cloud architecture

- Deploy apps and data across multiple cloud providers.
- Maintain consistent application delivery and security policies.
- Automated failover and server/container scale-out.
SOLUTION

Multi-cloud resilient architecture
Breach Visibility and Reporting

Solutions
Security of Processing

Article 32

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

   a) the pseudonymization and encryption of personal data;

   b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

   c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

   d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.
GDPR Breach Visibility and Reporting

**GDPR CHALLENGE**

Organisations must **report** breaches within 72 hours.

- Encrypted traffic can limit visibility into a breach.
- Inability to utilise all security products for SSL/TLS visibility (inline, offline, network tap).
- Multiple points of control for SSL/TLS.

**SOLUTION**

SSL orchestrating architecture

- Security service chaining.
- A centralised point of control that provides visibility for encrypting or decrypting data.
GDPR CHALLENGE

Efficiently report on breaches when traffic is encrypted.

Administrators are forced to choose: Let traffic go uninspected or suffer extreme application performance losses.
SOLUTION

SSL/TLS decryption for breach visibility

SSL Orchestrator

- Decrypt
- Re-encrypt

- Network tap (Long term capture)
- ICAP (DLP)
- L2 (IPS)
- L3 (NGFW)
Service chaining: Intelligent traffic management and decryption
Despite the opportunities to business, the risks may prevent deployment of new products.

- Adequate security may require new technology with deep understanding.
- The more comprehensive a security policy, the more complex it is to manage and maintain.
- Awareness and understanding of new and emerging vulnerabilities and attacks is hard to keep on top of.

Share risk by outsourcing complex security solutions.

- Experienced F5 security engineers develop and maintain security policies on your behalf.
- Deep analytics and visibility into attacks and mitigations used to prevent breach.
- Hosted cloud security may be used across many more apps than just the few mission-critical ones.
F5 Security Operations Center

SOLUTION

Dedicated SOC Engineers

Expert in WAF and DDoS Mitigation

24x7 Support

Active Threat Monitoring
Recommendations for Compliance in the Cloud

**Consistent Security**
- For all apps
- For all APIs
- On-prem
- Multi-cloud

**Visibility**
- Protocols
- **Encryption**
- Traffic patterns
- Server health
- Credential misuse
- Client device behavior

**Measurement**
Audit, report, and alert on...
- Suspected attacks
- Inconsistent policies
- Performance and attacks over time
- Consistent metrics across cloud providers

**Certification**
- Recognised framework
- ISO, CSA, CISPE, etc.
- Self-certification
- Due-diligence with CSA Matrix
- Look for external certification
Thank You