Security and Privacy Incident Response at Ericsson

Thomas Grenman
Ericsson PSIRT

TEAM BACKGROUND
Team established in 2004
Accredited by Trusted Introducer (GEANT/TF-CSIRT) in 2005
Full membership in FIRST since 2006
Main organization located in Finland
Current team size 1+13

MAIN OPERATIONS
Vulnerability management (monitoring and alerting)
Product security assurance
  • risk assessments
  • privacy impact analysis
  • security and vulnerability assessments
Development and maintenance of assessment methodology and tools
Triage and product related incident response
Tier-2 support for security issues raised by customers

FIGURES
Products and services deployed in over 180 countries
Our managed networks serving over one billion subscribers
Tracking vulnerabilities in close to 500 active products
17,000+ vulnerabilities analyzed yearly
3,000+ vulnerabilities registered yearly in vulnerability database

COOPERATION
Active cooperation with national / international CERT communities
Contacts established with vendor and operator CSIRT teams
Participating in EU Commission workgroups
Contributing to ETIS
Privacy Risk Heatmap

https://maplecroft.com/portal/#/portal/aod/scorecards/index/right_to_privacy/map
Incident Handling Flow

• The incident process cover everything from identification of a reported case up to closure and follow up of the final incident report

• Customers rarely report incidents directly to PSIRT, instead they file support cases

• The first step of the handling process is to determine if the incident is product related and if privacy aspects need to be taken into account

• Potential privacy incidents with activate the privacy officer(s) and trigger a subprocess for determining Ericsson’s relationship to the Data Subjects
Privacy and Security Incident Relationship

Protecting information from unauthorized access, disclosure, modification or destruction

Respecting a fundamental right to the protection of personal data
Incident Triage

• Appoint an incident lead
• Verify and record provided initial information
• If applicable, support in assessing the privacy impact
• Identify the urgency and criticality in order to prioritize the case
• Create a response strategy plan (and keep it updated)
• Identify and handshake with essential stakeholders (e.g., administrators, technical experts, KAMs, service delivery manager, privacy officers, etc.)
• Determine the need to preserve forensic evidence
• Clarify the outcome and the expectations of the incident investigation
Privacy Incident vs. Privacy Breach

- An incident happened
  - Personal data compromised
    - Likely to impact data subjects
      - Remediation possible
        - Privacy breach
      - Privacy incident
        - Severe privacy breach
    - Not a privacy incident
Incident Communications

- Keep stakeholder up-to-date during investigation
  - regional service delivery managers
  - involved product organization
  - customer

- Additional communications for privacy incidents
  - approve all communications through appointed privacy officer
  - depending on the local legislation, communicate with DPA, other public authorities and directly with data subjects (if needed)

- If needed, PSIRT will assist in formulating a privacy breach notification
Common Causes of Privacy Incidents

• Lack of security controls
  • loss of equipment containing data
  • transfer, sale or disposal of equipment containing data (without wiping it first)
  • use of equipment without adequate transfer or storing protection for data
  • failing to protecting against intrusion into equipment containing data
  • insufficient rights to access or modify data (e.g., wrongful access, tampering)
  • inadequate security or access controls for data in print or electronic format
  • processing data without or in contradiction with consent
Common Causes of Privacy Incidents (cont.)

• Lack of privacy controls
  • low privacy awareness and data handling competence within staff, contractors and third parties
  • lack or inadequate provisions to protect privacy in contracts or in agreements on processing and information sharing
  • lack of data recognition
  • transfer of data outside country without adequate protection measures
  • lack or privacy processes or policies at Data Controller's or Processor's end
  • lack of policy implementations or consent management in product, services, and operations
Security and Privacy by Design

SECURITY AND PRIVACY RELIABILITY MODEL
Baseline Requirements for Products and Solutions

FUNCTIONS
ASSURANCE
DOCUMENTATION
SECURITY AND PRIVACY SERVICES

PRODUCT DEVELOPMENT
CUSTOMER DELIVERY
Implementation Examples
Baselined Logging and Data Tagging

• A minimum criteria for logging
  • **Who** accessed personal data
  • **When** was the data accessed
  • **What actions were performed** on the data
  • **Data item tags** applied to personal data

<table>
<thead>
<tr>
<th>Data Item</th>
<th>Tag</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSISDN</td>
<td>[1]</td>
</tr>
<tr>
<td>IMSI</td>
<td>[2]</td>
</tr>
<tr>
<td>IMEI</td>
<td>[3]</td>
</tr>
<tr>
<td>Location (Other)</td>
<td>[6]</td>
</tr>
<tr>
<td>IP-address</td>
<td>[7]</td>
</tr>
<tr>
<td>First Name</td>
<td>[8]</td>
</tr>
<tr>
<td>Last Name</td>
<td>[9]</td>
</tr>
<tr>
<td>…</td>
<td></td>
</tr>
</tbody>
</table>
Implementation Examples (cont.)

Pseudonymization of Log Files

Normal log file in plain text

[Mon 2017-05-29 13:37:00 +0300] Received purchase request from user [1:123]smith
[Mon 2017-05-29 21:31:46 +0300] Received purchase request from user [1:456]johnson
...

De-identified log file with format preserving encryption

[Mon 2017-05-29 13:37:00 +0300] Received purchase request from user [1:123]aqugj
[Mon 2017-05-29 21:31:46 +0300] Received purchase request from user [1:456]omqnfjh
...
Key Takeaways

• As a Data Controller or Data Processor
  • know the data, know where it is stored, know the local legislation
  • have (rehearsed) processes in place, have well-defined responsibilities
  • agree on communications channels, get to know the local DPA, agree on templates (e.g., breach notification)
  • avoid making contracts that can block or slow down your investigation
  • transfer legal liability for data protection to parties involved in data processing
  • employ forensic investigators or keep a shortlist of local third parties that quickly can aid with needed technical investigation
  • have the technical capability to notify victims (potentially in the millions)
Key Takeaways (cont.)

• As a technology provider
  • identify and document personal data being processed by the product
  • have requirements in place to ensure that the product privacy impact is assessed
  • implement needed technical features to
    • allow classification of personal data according to local regulation and law
    • ensure high data quality (allow updating or deleting outdated information)
    • enable data de-identification, anonymization, and scheduled erasures acc. to retention times
    • enable data transfers (through machine-readable exports and imports)
    • allow fine grained access controls to all processed data item
    • protect confidentiality and integrity of personal data at rest and when in transfer
    • collect sufficient logging (i.e., audit trails) for all vital privacy related events
Thank You!