Security service provisions

EDPS-ENISA Conference

Towards assessing the risk in personal data breaches

Brussels, 4th April 2019

Giampiero Nanni

Government Affairs – EMEA
giampiero_nanni@symantec.com
+44 780 8248100

Essential tools & processes for prevention and handling of personal data breaches

Symantec

PREPARE

Risk Assessment

- Identify Threats & Vulnerabilities
- Data and critical asset mapping (including in Cloud)
- Governance and risk management processes
- Asset & supply chain dependencies
- Data subject risk

RECITAL 75

TOOLS

- ✓ Cyber Intelligence tools, custom intel
- ✓ Compliance assessment and tracking
- ✓ Security Analytics, Endpoint detection, SIEM, Intelligent threat prioritisation and alerting, Machine behaviour analysis, Malware analysis, Proxi, Data Centre risk management & platform protection, Network forensic tools

PROTECT

Protecting Against Personal Data Loss

- Malware protection
- Advanced Persistent Threat protection
- Insider threat protection
- Personal Data protection, in motion, in use, at rest
- Network, system and data security

ALMOST NO EXCUSES

- ✓ Encryption
- ✓ Pseudonymisation
- ✓ Cloud Access Security Broker (CASB)
- ✓ Data loss prevention
- ✓ Access governance
- ✓ Authentication
- ✓ Intrusion prevention
- ✓ Encrypted traffic management
- ✓ Malware protection
- ✓ Zero-Trust
- ✓ Web Isolation

DETECT

Detection capabilities

- Multiple Stakeholders, including non-tech
- Continuous monitoring, proactive event discovery
- Real time breach detection on premise & cloud
- Reduced detection time→Reduced damage severity

- ✓ Events correlation tools (e.g. SIEM)
- ✓ Full incident information for notification (e.g. security analytics tools can demonstrate that data was encrypted hence unusable by thieves)

RESPOND

Response process

- Capability (skills, response plans, technology)
- Contain the incident, remediate
- Ensure ops continuity. Restore initial status. Resilience
- Learn from the incident

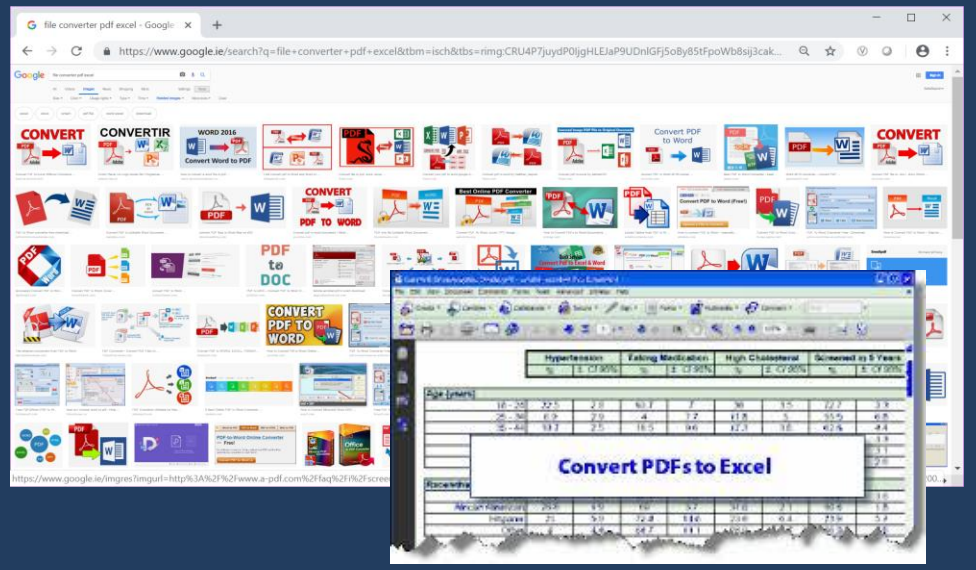
- ✓ Communication and notification processes
- ✓ Security analytics (e.g. to document measures taken to mitigate an incident)
- ✓ Relevant notifications
- ✓ (Automated) Security posture improvement

Shadow IT & Shadow Data: A recipe for non-compliance and data subject risk

- **Shadow IT**: Unsactioned Apps in the Cloud, accessed or downloaded, and used by the employees without knowledge of the IT Dept.
- **Shadow Data:** Data processed by Shadow Apps.
- Our studies show how IT depts believe that the number of Apps run in the company in the Cloud are on average 30-40. We found out that they are rather in the region of 1,000+, as employee are very active downloading unsanctioned ones
- **The questions are:** What do employees do with these apps? What data do they process? And in particular what Persona Data?

Use case

Employees need to convert PDF files into Excel.
There are numerous free Apps or websites that will do that.
In this case the instructions tell the user to UPLOAD the PDF, and then to DOWNLOAD the resulting Excel.
Besides the risk of downloading items that could be infected, the big risk is with Personal Data being uploaded on some unknown Website.
The potential risks from a GDPR compliance point of view are in the next slide.



How to convert PDF to Excel sheets online

1. Upload your file to our **PDF to Excel Converter**.
2. If the file is a scan, OCR will activate automatically.
3. Wait as Smallpdf **converts** the file to **Excel**format.
4. Click 'Download' to save your newly **converted Excel** file.

PDF to Excel Converter - 100% Free - Smallpdf.com
https://smallpdf.com/pdf-to-excel

Shadow IT & Shadow Data: Potential infringements to the GDPR

- The way data flow inside and outside the already fragmented boundaries of the organisation;
- The use of the personal data, by which actors, internal and external, and whether they are authorised to process them;
- The knowledge of which processes are executed by these shadow apps, over which personal data - By definition, these processes will be unlikely to have been recorded and documented, as required by **Article 30** for organisations with more than 250 employees;
- The need to know who the processor of the data is, with the related implications, namely a proper processor breach notification process, including Data Breach Detection And Notification (**Articles 33 and 34**) - In a similar scenario the most likely outcome is that the data breach is discovered when the personal data involved is leaked widely, e.g. over the web;
- The security provisions for the personal data used by these shadow apps – In accordance with **Article 5(f)** and **Article 32**
- The principles of Purpose Limitation, Storage Limitation, Confidentiality and Integrity (**Article 5**);
- The obligations of Data Protection by Design and by Default, as per **Article 25**, as well as any accountability requirement.
- The obligations regarding the lawfulness of processing (**Article 6**);
- The duties regarding transparency (**Articles 12-14**) and data subject rights (**Articles 15-21**);
- The requirements of cross-border data transfers (**Chapter V**) – Shadow apps could be operated and hosted by providers in Countries outside the EEA, with unverified adequacy;
- The risks deriving from joint controllership (**Article 26**)
- The Processor obligations and sub-processing (**Article 28**) as well as the controller-processor relationship (**Article 29**)
- In case of high-risk processing , Risk Assessment, DPIA Accuracy, Prior Consultation (**Articles 35-36**)
- Ultimately, a Shadow IT situation will impede the overall accountability of the organisation (**Articles 5 & 24**)

Security service provision

EDPS-ENISA Conference
Towards assessing the risk in personal data breaches
Brussels, 4th April 2019

Giampiero Nanni

Government Affairs – EMEA
giampiero_nanni@symantec.com
+44 780 8248100