Engenharia de Segurança

Aula 7 - 19/03/2018

Afonso Fontes (pg35389)
Bruno Carvalho (a67847)
Mariana Carvalho (a67635)

26 de Março de 2018

Universidade do Minho

RGPD (Regulamento Geral de Proteção de Dados)

Pergunta 1.1

No artigo 32º do RGPD são referidas as medidas técnicas e organizacionais que devem ser implementadas de forma a assegurar um nível de segurança apropriado, face à sensibilidade e ao nível de risco associado aos dados que são tratados. Este artigo também especifica que devem ser tomadas medidas que garantam que qualquer pessoa que tenha acesso a dados pessoais de terceiros, só possa processar os mesmos mediante a instrução do responsável do tratamento, ou exceto se tal lhe for exigido pelo direito da União ou de um Estado-Membro. De forma a atuar em conformidade com o regulamento, as medidas de segurança aplicadas devem:

- Assegurar **pseudonimização** dos dados pessoais, através da substituição dos campos identificadores dos titulares dos dados (toda a informação que permita identificar direta ou indiretamente o titular) por identificadores artificiais, ou pseudónimos, e quando possível, a cifragem dos mesmos;
- Garantir **confidencialidade**, **integridade**, **disponibilidade** e **resiliência** contínua dos sistemas e serviços, isto é, garantir que todos os dados estão disponíveis para os utilizadores, e que são tomadas provisões que garantam que os dados não são adulterados por terceiros, que acidental ou propositadamente ;
- Em caso de eventos imprevistos, sejam estes incidentes físicos ou técnicos, assegurar que o acesso aos dados pessoais seja **rapidamente restaurado**, o que implica backups remotos e planeamento prévio de estratégias de emergência;

As organizações devem implementar processos de teste, apreciação e avaliação regular das técnicas implementadas de forma a garantir que estas cumprem o seu propósito e funcionam como planeado. Dependo do contexto, estes processos podem variar entre recorrer a ferramentas de segurança, como scanners para vulnerabilidades web e ferramentas de monitorização, para políticas de password fortes e até um rigoroso processo de contratação ou treino de funcionários, para que estes se encontrem ao corrente das mais recentes tecnologias.

Adicionalmente, o artigo 32º refere que as organizações devem considerar os riscos associados ao tratamentos de dados pessoais, destacando-se a destruição, perda e alteração acidentais ou ilícitas, e à divulgação ou ao acesso não autorizados, de dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento e por isso só permitir a manipulação de dados a pessoal autorizado.

Em suma, as organizações devem garantir que todos os dados pessoais tratados são guardados de forma segura e a sua transmissão está restrita a indivíduos de confiança, ou com autorização.