Definição dos tópicos essenciais sobre segurança na internet, diferenças entre países

BE SAFE ON THE INTERNET

Co-funded by the Erasmus+ Programme of the European Union

Índice

1. Introdução

Atualmente grande parte da informação encontra-se *online* e quase todas as atitudes dos cidadãos tem algum impacto na internet (redes sociais, e-mails, transferências monetárias, *cookies*, etc.).

Além disso, nos dias de hoje, quase tudo tem uma ligação direta na internet graças à quarta revolução industrial - e isto é só o princípio.

O principal objetivo deste relatório é sintetizar as conclusões mais importantes tendo em conta duas temáticas: cibersegurança / segurança na internet e dados pessoais / segurança na internet.

Adicionalmente, e tal como vimos no relatório anterior, há diversas semelhanças nos países envolvidos neste projeto de acordo com as temáticas referidas anteriormente. Assim, as diferenças existentes entre estes países estão mais relacionadas com algumas questões que ainda se encontram em aberto que permitem aos legisladores algum poder de decisão.

2. Principais conclusões

Neste capítulo temos uma lista das principais conclusões retiradas do Resultado n.º *2* - Aspetos legais sobre segurança na internet do projeto. As conclusões estão divididas em dois temas.

2.1. Cibersegurança e segurança na internet

2.1.1. Trabalho/empresas

- Os ataques são cada vez mais complexos e frequentes e a principal motivação destes ataques está relacionada com questões financeiras;
- A segurança na nuvem é um aspeto cada vez mais crítico e as empresas tendem a ficar mais dependentes dos fornecedores de serviços de armazenamento de dados (servidores);
- A importância de possuir medidas de organização (p.e. gestão de risco) irá crescer no futuro comparativamente com a utilização de medidas exclusivamente técnicas;
- A dependência das empresas relativamente a produtos de *hardware* e *software* representa uma ameaça crescente;
- Não existem incentivos suficientes para o investimento em segurança por parte das empresas;
- Falta de consciencialização para a segurança e padrões de comportamento assertivos;
- Existência de legislação obsoleta ou ausência de sustentação legal em diversos países, algo que dificulta a compreensão e a aplicação de medidas de segurança;
- Falta de conhecimento sobre segurança por parte da maioria das pessoas;
- Falta de pessoal qualificado e carência de competências técnicas na área de cibersegurança;
- Falta de oferta de formação que vise a melhoria do conhecimento e do comportamento sobre segurança por parte das pessoas;

- Falta de consciencialização por parte dos trabalhadores face às ameaças cibernéticas e desconhecimento das regras de segurança na utilização das tecnologias de informação (TI);
- Falta de uma orientação técnica clara e concisa relativamente à cibersegurança e segurança na internet;
- As exigências salariais crescentes do pessoal qualificado e especializado em cibersegurança podem dificultar o combate a este problema;
- A diversidade de ferramentas existentes tem contribuído para o aumento da complexidade operacional deste desafio e dificultado a visibilidade de uma postura geral de segurança;
- As organizações não têm por norma uma equipa responsável ou mesmo um técnico especializado que responda prontamente a incidentes relacionados com cibersegurança;
- Falta de colaboração entre as equipas de cibersegurança;
- Muitas empresas não têm um plano de resposta consistente face à maioria dos problemas de cibersegurança;
- Falta de tempo e de recursos qualificados necessários à implementação de um plano de cibersegurança;
- Falta de um orçamento adequado para aumentar os recursos alocados à segurança;
- Utilização de *hardware* e *software* obsoleto;
- Falta de compromisso por parte dos órgãos de gestão bem como orçamentos insuficientes;
- Falta de envolvimento dos trabalhadores na estratégia de cibersegurança da empresa (se esta existir);
- Os recursos materiais e físicos existentes relacionados com a cibersegurança não são do total conhecimento de todos os trabalhadores na empresa;
- A cultura de cibersegurança necessita de ser assimilada por toda a equipa de trabalho nomeadamente através de programas de segurança, de uma gestão e prevenção do ambiente e risco laboral e introdução de medidas e processos e gestão;
- Existência de poucas iniciativas com foco na cibersegurança industrial;

- As soluções de cibersegurança existentes ainda não foram suficientemente testadas;
- Falta de cooperação entre as empresas e o governo;
- Comunicação ineficiente entre as equipas de trabalho devido às diferenças de conhecimento e competências existentes relacionadas com *hardware* e *software*;
- Existem atividades que podem pôr em perigo os sistemas e, consequentemente, a segurança dos processos industriais e das instalações;
- Falta de sensibilização para os efeitos e para a necessidade de introduzir novas tecnologias para assegurar a operacionalidade dos sistemas de controlo;
- Perceção geral de que as ameaças existentes são algo incerto e bastante improvável;
- A espionagem através de recursos digitais modernos ameaça a competitividade nacional e a produtividade;
- Existência de diferentes necessidades de cibersegurança de acordo com os diferentes setores de atividade;
- Falta de apoio financeiro para o desenvolvimento da cibersegurança;
- Escassez ou inexistência de padrões específicos para a cibersegurança;
- Incompreensão desta temática devido à escassez de programas de formação específicos e de material de comunicação;
- Falhas na implementação de soluções de segurança e tecnologia como *firewalls*, soluções *Intrusion Detection System* (IDS)/ *Intrusion Prevent System* (IPS), antivírus, etc;
- Inexistência de cooperação institucional ou de acordos entre as entidades públicas competentes, empresas e fornecedores do setor da cibersegurança;
- Coordenação deficitária entre os estados membros da União Europeia (UE).

2.1.2. Vida privada

- Falta de sensibilidade para as questões da segurança;
- Existência de comportamentos negligentes na utilização da internet;
- Os programas curriculares do ensino superior não incluem na maior parte das vezes as temáticas da cibersegurança;

- Apesar de existirem boas iniciativas, dicas e sugestões sobre o tema, estas não chegam à maioria da população;
- Elevado número de programas de *software* malicioso no mercado;
- Falta de compreensão relativamente ao estatuto dos ciber-ataques;
- Existem muitas zonas rurais onde não existe uma oferta formativa adequada devido à localização geográfica;
- O apoio aos utilizadores afetados e o esclarecimento de dúvidas está, regra geral, disponível através de telefone ou *online* exceto se o utilizador se dirigir diretamente à polícia. Nestes casos é necessário a existência de um meio de contacto direto, onde as pessoas se possam dirigir pessoalmente caso tenham algum problema;
- Os regulamentos, políticas e leis não são facilmente percetíveis pelos utilizadores comuns;
- A informação que consta nos materiais de apoio nem sempre é de fácil acesso e, por este motivo, esta deverá ter um acesso rápido e intuitivo;
- Utilização de uma senha de acesso frágil, uma única senha de acesso para múltiplas plataformas e utilização de senhas sem alteração regular das mesmas;
- Falta de conteúdos académicos e científicos sobre cibersegurança;
- As pessoas confiam facilmente nos anexos do seu e-mail;
- As pessoas partilham muita informação pessoal nas redes sociais;
- Desinteresse generalizado do público mais jovem sobre questões de segurança na internet;
- Falta de sensibilização para as ameaças do ciberespaço e para as regras de segurança relacionadas com a utilização das TI;
- Não existem muitas plataformas sobre cibersegurança para partilha de informação;
- Falta de apoio financeiro para a promoção da segurança na internet junto das pessoas e para o desenvolvimento de novas soluções;
- Poucas iniciativas subordinadas ao tema da segurança na internet no nosso dia-a-dia;
- Escassez de programas de educação e formação, bem como materiais pedagógicos relacionados com a segurança na internet;

- Baixa literacia digital por parte dos utilizadores;
- Falta de conhecimentos básicos sobre potenciais ameaças por parte das entidades e serviços públicos;
- Não está criada uma cultura de cibersegurança;
- Falta de uma orientação clara e concisa sobre segurança na internet e cibersegurança;
- Os recursos existentes ligados à cibersegurança não são plenamente conhecidos;
- Falta de sensibilização para os efeitos e para a necessidade de adoção de novas tecnologias que assegurem a operacionalidade dos sistemas de controlo;
- Incompreensão da cibersegurança e da segurança na internet devido à escassez de programas de formação específicos e de ferramentas de comunicação de iniciativa pública;
- As políticas e os procedimentos existentes não são adequados do ponto de vista da cibersegurança;
- Os riscos da cibersegurança não estão integrados em ferramentas e sistemas;
- Ainda não existem soluções de cibersegurança devidamente testadas;
- Falhas na implementação de soluções de segurança e tecnologia como *firewalls*, soluções IDS/IPS, antivírus, etc;
- Coordenação deficitária entre os estados membros da UE.

2.2. Proteção dos dados pessoais e segurança na internet

- As novas regras relacionadas com a proteção dos dados pessoais implicarão exigências adicionais às empresas;
- Existe ainda uma fundamentação legal obsoleta e um conjunto de informações que dificultam a compreensão e a implementação do Regulamento Geral de Proteção de Dados (RGPD) e a demais legislação sobre proteção de dados pessoais;
- Existência de divergências no que toca à informação, medidas e procedimentos necessários à implementação adequada do RGPD deve-se ao facto de existirem muitas empresas que continuam sem saber o que realmente têm de fazer;
- Necessidade de aceder facilmente à informação de forma simples e clara;

- Implementação frágil ou inexistente de medidas para aumentar a proteção dos dados pessoais no dia-a-dia;
- Falta de medidas, sugestões e acesso a formação sobre proteção de dados pessoais adequada para qualquer pessoa independentemente da idade, conhecimentos ou localização geográfica;
- Falta de atividades de formação desde faixas etárias mais jovens;
- Desenvolvimento da cidadania digital do estudante através de tecnologia apropriada, incluindo comunicação *online* e direitos digitais e responsabilidades;
- Os europeus necessitam de uma maior proteção da sua privacidade *online*;
- Diversas empresas ainda reconhecem a necessidade de reforçar a informação e a formação dos colaboradores relativamente ao RGPD;
- A maioria das empresas necessita de uma primeira avaliação para avaliar o nível de conformidade e a adequação às políticas e processos correntes para uma correta identificação da necessidade de possíveis alterações que cumpram com o RGPD;
- Os atuais desafios relacionados com a modernização, globalização, tecnologia e digitalização implicam uma revisão do processo do RGPD;
- Criar um compromisso com toda a comunidade envolvida com as questões da proteção de dados pessoais logo que possível;
- Definir e rever, com regularidade, o conhecimento, as competências, os atributos e outras características que as pessoas podem adquirir e aprofundar de acordo com as temáticas abordadas;
- Estimular a produção de conteúdos criativos e pedagógicos simples e acessíveis para a comunidade em geral;
- As tecnologias digitais estão em constante evolução e os professores/formadores necessitam de receber formação constante para que sejam capazes de apoiar e desenvolver formações adequadas aos seus públicos;
- Distribuição de responsabilidades pelas equipas de trabalho acerca da proteção de dados pessoais;
- Manter a documentação detalhada acerca dos dados recolhidos nomeadamente como é utilizada, onde é armazenada, qual o colaborador responsável pela informação, etc;

- Disponibilizar formação à equipa e implementar medidas de segurança (técnicas e organizacionais).

2.3. Cibersegurança na Europa

Durante os últimos anos a Comissão Europeia (CE) implementou uma série de medidas alternativas para assegurar um ambiente *online* mais seguro na UE e encontra-se a desenvolver esforços para aumentar a capacidade e a cooperação existente no âmbito da cibersegurança, fortalecendo assim a UE e tornando-a uma referência no mundo nesta temática.

Desde 2017, a UE iniciou um compromisso relacionado com a implementação de medidas de cibersegurança que reforçam o aumento da confiança dos cidadãos e das empresas na sociedade digital europeia mas foi apenas em julho de 2019 (com o regulamento (UE) 2019/881 do Parlamento Europeu) que foram implementadas uma série de medidas que tem como objetivos promover a cibersegurança na UE e a segurança do ambiente digital na Europa. Além disso, o "*European Cybersecurity Act*" é uma parte do projeto geral de cibersegurança da UE que estabelece requisitos de segurança e a existência de notificações para os operadores de serviços e fornecedores de serviços digitais tais como os operadores de serviços de armazenamento na nuvem.

Desde junho de 2019, e com o "*European Cybersecurity Act*" marcou também o novo mandato da European Union Agency for Cybersecurity (ENISA), a agência para a cibersegurança da UE que estabeleceu a estrutura de certificação europeia da cibersegurança.

Apesar de já existir alguma legislação em vigor sobre cibersegurança nos estados-membros existem também algumas questões legais em aberto que permitem alguma margem de manobra aos legisladores nacionais para a implementação da cibersegurança. Em alguns países europeus (nomeadamente na República Checa, Áustria, Portugal e Espanha) existe legislação/diretivas/códigos que abordam as questões da cibersegurança nos seus territórios. No entanto, os regulamentos da cibersegurança ainda carecem de um desenvolvimento mais profundo isto porque o Parlamento Europeu atua como colegislador e são os próprios estados-membros os principais responsáveis

pela sua própria cibersegurança. Como tal, é necessário implementar algumas medidas com o objetivo de reforçar a ciber-resiliência tais como:

- A legislação da cibersegurança mantem-se incompleta e há alguns atrasos sobre esta temática no território europeu. Como tal, é necessário melhorar a partilha de informação e a coordenação entre os legisladores e os setores público e privado terão de trabalhar em conjunto para poder responder aos desafios da cibersegurança num futuro próximo;
- Os agentes políticos e legisladores têm de criar legislação mais simples e clara que seja percetível por todos os cidadãos independentemente da sua origem ou habilitações;
- De acordo com o relatório do Tribunal de Contas Europeu "Desafios para uma política eficaz de Cibersegurança da UE", 80% das empresas da UE já vivenciaram, pelo menos uma vez, um incidente de cibersegurança em 2016; 69% não tem ou têm apenas algumas noções básicas sobre a sua exposição a ciber-ataques e 60% nunca estimaram os potenciais prejuízos de um ciber-ataque. Por esta razão, a cibersegurança nas empresas terá de ser uma prioridade e, neste contexto, deverá ser alvo de auditorias ou análises externas regulares (p.e. uma vez por ano). Com estas auditorias, as organizações terão acesso a informação bastante útil e irão conhecer quais os aspetos que necessitam de ser trabalhados/melhorados. Neste sentido, as empresas têm a responsabilidade de implementar ações com o objetivo de garantir boas práticas sobre cibersegurança;
- A legislação só por si não garante a resiliência e para criar uma cultura de ciber-resiliência cada empresa deve ter um plano pró-ativo e reativo que responda aos incidentes relacionados com a cibersegurança;
- É necessário ter uma perspetiva geral sobre as necessidades de formação e as fragilidades de cada pessoa no que toca a esta temática. Portanto, o aumento das competências e a sensibilização das pessoas logo desde o início é obrigatório e deve iniciar o mais rápido possível em cada país. Por exemplo, é importante organizar algumas iniciativas e implementá-las nas empresas, escolas ou até em casa. De acordo com estas sugestões, por exemplo, as empresas deverão ter nos seus quadros uma pessoa qualificada/certificada na área da cibersegurança que possa dar formação aos restantes membros da equipa, especialmente na área do

software como por exemplo: ataques de *phishing*; *malware*; cavalos de tróia; *spam*; *ransomware* roubos de dados. Estas formações também são importantes para desenvolver uma cultura de cibersegurança.

Todas as sugestões mencionadas anteriormente pretendem alcançar um maior nível de cibersegurança na UE e uma resposta mais eficaz perante os incidentes cibernéticos.

3. Catálogos de conteúdos sistematizado

Os aspetos mais importantes sobre os dois temas analisados no Resultado n.º 2 estão descritos a seguir:

- **Segurança na nuvem:** também conhecida como segurança na *cloud* a segurança na nuvem consiste num conjunto de políticas, medidas, procedimentos e tecnologias que atuam de forma cooperativa para proteger os sistemas, dados e infraestruturas armazenados na nuvem. Estas medidas de segurança são configuradas para proteger os dados, cumprir com a legislação em vigor, proteger a privacidade dos utilizadores/clientes e definir regras de autenticação para utilizadores individuais e dispositivos;
- **Cibercrime:** qualquer atividade criminosa que envolva um computador, um dispositivo ligado em rede ou uma rede informática. Enquanto a maioria dos cibercrimes são realizados para obter benefícios financeiros aos criminosos, alguns cibercrimes são realizados em computadores ou outros dispositivos com o intuito de os destruir, desativar ou difundir *malware*, informação ilegal, imagens ou outros materiais. O cibercrime pode abranger diferentes tipos de crimes com fins lucrativos incluindo ataques de *ransomware*, e-mail, operações fraudulentas na internet, identidades falsas *online*, roubo de dados bancários e dos cartões de crédito ou outros meios de pagamento;
- **Cibersegurança:** inclui atividades de proteção de sistemas, redes informáticas e programas por parte de ataques digitais; estes ciber-ataques pretendem normalmente aceder, alterar e destruir informação crítica, extorquir dinheiro dos utilizadores ou simplesmente interferir em processos comerciais normais;
- **Ciber-roubo:** roubo de informações pessoais e/ou financeiras através de computadores para utilização fraudulenta ou ilegal;
- **Violação de dados:** divulgação intencional ou não intencional de informação protegida ou privada/confidencial junto de ambientes não confiáveis. A violação de dados pode envolver informações pessoais de saúde, informação pessoal que identifique facilmente a pessoa, segredos comerciais e/ou propriedade intelectual;
- **Fuga de informação:** transmissão de informação não autorizada (fisicamente ou

por via digital) de uma organização para um destino externo. As potenciais fugas de informação ocorrem normalmente por internet e por e-mail mas também ocorrem através dispositivos móveis de armazenamento de dados como discos externos, *pen drives*, computadores portáteis, etc;

- **Proteção de dados:** processo de proteção de informação que envolve a relação entre a recolha e disseminação de dados e tecnologia, a perceção pública e a expectativa de privacidade e os fundamentos político-legais em torno desses dados. O objetivo passa por alcançar o equilíbrio entre o direito à privacidade individual e a possibilidade de utilizar os dados pessoais para fins comerciais;
- **Privacidade da informação:** a privacidade de informação é um ramo da segurança de dados que se preocupa com a manipulação de dados - consentimento, notificação e obrigações regulamentares. Mais especificamente a segurança dos dados está relacionada com preocupações práticas com dados privados: se ou como os dados são partilhados com terceiros; como são recolhidos ou armazenados os dados legalmente e restrições regulamentares (p.e. RGPD);
- **Segurança dos dados:** um conjunto de padrões e tecnologias que protegem os dados de serem destruídos, modificados ou divulgados de forma intencional ou acidental. A segurança de dados pode ser aplicada usando um conjunto de técnicas e tecnologias, incluindo controlos administrativos, segurança física, controlos lógicos, processos padronizados e outras técnicas de proteção que limitam o acesso a utilizadores e processos não autorizados ou mal-intencionados;
- **Segurança na internet:** maximização da segurança pessoal do utilizador e dos riscos associados relativamente à informação privada e propriedade intelectual na internet incluindo a autoproteção contra crimes informáticos no geral;
- ***Malware*:** qualquer programa ou ficheiro que seja perigoso para o utilizador de um computador. Alguns exemplos de *malware* incluem vírus informáticos, programas com vírus, cavalos de tróia e *spyware*. Estes programas maliciosos conseguem desempenhar diversas funções como apagar, roubar ou encriptar informação importante, alterar ou manipular funções centrais do computador e monitorizar atividade informática dos utilizadores sem qualquer permissão;
- ***Phishing*:** forma de fraude onde um pirata informático se faz passar por uma

entidade ou pessoa através de um e-mail ou outro canal de comunicação alternativo. O pirata usa estes e-mails *phishing* para distribuir *links* ou anexos infetados que podem desempenhar diversas funções prejudiciais no computador de outra pessoa como por exemplo extrair credenciais de acesso, palavras-passe ou informações das contas das vítimas;

- **Violação de segurança:** qualquer incidente que resulte de um acesso não autorizado a dados, aplicações, serviços, redes e/ou dispositivos ignorando os mecanismos de segurança adjacentes. Uma violação de segurança ocorre sempre que um indivíduo ou um programa acede de forma ilegítima a informações do foro privado, confidencial ou não autorizado;
- ***Spam*:** sistemas de mensagens eletrónicas enviadas de forma massiva sem autorização ou sem qualquer solicitação por parte dos recetores. A forma mais comum de *spam* é um e-mail *spam* mas este termo também se aplica a qualquer mensagem enviada eletronicamente e em massa sem que a mesma seja solicitada;
- **Cavalo de tróia:** *software* malicioso que é normalmente disfarçado num *software* legítimo. Os cavalos de tróia podem ser infiltrados por *hackers* que tentam aceder aos sistemas dos usuários;
- **Vírus:** tipo de código ou programa malicioso programado para alterar a forma como o computador opera e é concebido para se expandir de um computador para outro.