JF MAIS TIC

“Segurança nacional deve passar pela terra, mar, água e Internet” Manuel Lopes Rocha
| P. III

Consórcio investe 5,5 milhões em projeto de segurança?IoT?
| P IV e V

Cibersegurança e privacidade dos dados

O novo mundo em que vivemos é, cada vez mais, digital, colocando novos desafios e trazendo novos riscos. Neste Especial, falamos sobre a cibersegurança, questão transversal que respeita a cidadãos, a organizações e aos Estados. Também sobre proteção de dados, quando falta cerca de um ano para a entrada em vigor do novo regulamento. E de como tudo começa em nós, hoje, por exemplo, no dia mundial da password.

David Becker/Reuters

OPINIÃO

BYOD nas empresas: um problema de segurança

ALFONSO RAMÍREZ
diretor-geral Kaspersky Lab Iberia

Os smartphones e os tablets são cada vez mais utilizados do que os próprios computadores, mesmo no contexto empresarial. Como tal, os hackers começaram a direcionar os seus ataques para estes dispositivos que reúnem uma enorme quantidade de dados pessoais e profissionais. Lamentavelmente, temos comprovado que a grande maioria não tem instalado nenhum software de segurança.

Esta tendência do Bring Your Own Device (BYOD) está muito presente no dia-a-dia das empresas, já que os colaboradores começaram a utilizar os seus dispositivos pessoais para efeitos de trabalho, como aceder ao e-mail da empresa através do seu smartphone ou tablet pessoais. O mesmo pode acontecer em sentido inverso, ou seja, dispositivos da empresa que são utilizados para fins pessoais. O mais preocupante acaba por ser o facto de a grande maioria não estar consciente dos riscos presentes nesse processo ao nível da segurança, pondo em risco toda a rede corporativa. Destas práticas, podem resultar roubos de dados que afetem a empresa a nível económico e de reputação, por isso identificamos a proteção dos dados empresariais como uma prioridade.

As empresas devem estar atentas e conscientes destas novas práticas e dos possíveis problemas consequentes e devem ter em conta a formação e a consciencialização dos seus colaboradores para estes temas para que também possam deixar de ser o escalão mais débil da segurança corporativa.

Os melhores instrumentos de segurança de nada servirão aos seus colaboradores se estes não dispuserem de conhecimentos, mesmo que básicos, sobre como proteger a informação que guardam nos seus dispositivos.

Para garantir que o BYOD não prejudica o normal funcionamento das empresas, partilhamos uma série de recomendações que as empresas devem ter em conta na ligação de dispositivos pessoais às redes corporativas.

Para começar, a integração BYOD deve ser vista como um projeto específico, sobretudo quando se trata de grandes empresas. O processo de integração deve ser desenhado de antemão e deve incluir, idealmente, uma auditoria à infraestrutura, colocando a segurança como elemento fundamental do plano.

Num segundo momento é importante utilizar uma solução de segurança integral que proteja toda a rede corporativa, e não uma que se centre exclusivamente num único tipo de dispositivos.

Por último, é crucial que as empresas desenvolvam estratégias de atuação para desincorporar os dispositivos pessoais e/ou profissionais da rede da empresa em cenários de perda ou roubo dos dispositivos ou se um colaborador deixar a empresa. Este procedimento deve ser desenvolvido para eliminar os dados corporativos confidenciais destes dispositivos e bloquear o respetivo acesso à rede corporativa.

Percebemos que para além de uma segurança reativa perante os incidentes, é necessário que exista uma segurança proactiva na hora de planear uma estratégia de segurança eficaz contra as novas tendências cibercriminosas. Não devemos esquecer que a segurança não é um "estado", mas sim um processo. Devemos estar continuamente alerta, revendo e melhorando as nossas medidas.

O BYOD trás vantagens, mas também algumas desvantagens às empresas. Por um lado, permite uma redução dos custos, já que não existe a necessidade de comprar dispositivos móveis, tablets ou computadores para toda a equipa, uma vez que podem utilizar os pessoais.

Para os colaboradores traz a vantagem de não precisarem de ter dois dispositivos. Por outro lado, a maior desvantagem é a falta de segurança. E a questão que se coloca é: quem deve proteger o dispositivo?

A empresa ou o colaborador? Na verdade, a empresa é a que sai mais prejudicada, pelo que deve responsabilizar-se por proteger todos os dispositivos dos seus colaboradores a partir dos quais estes acedem a informações corporativas. No fundo, as empresas devem proteger todos os dispositivos que se conectem à sua rede corporativa já que com isso estão ao mesmo tempo a proteger-se a si mesmas.

TENDÊNCIAS

Evonic apresenta-se ao mercado, focada nas grandes empresas

A consultora tecnológica Evonic apresentou-se esta semana ao mercado com uma oferta centrada na transformação de postos de trabalho, automação, soluções de virtualização, DevOps e cloud híbrida, entre outras valências.

Em declarações ao Jornal Económico, Patrícia David, senior account manager da Evonic, explica que a empresa vai focar o seu negócio no segmento das grandes empresas, como a EDP – Energias de Portugal, a Vodafone, a Fidelidade ou a Caixa Geral de Depósitos (CGD).

A Evonic é subsidiária da RIS 2048, que é a sua principal acionista e tem duas décadas de atividade, mas é mais "generalista", focada em médias empresas.

A diferenciação da nova empresa passa "pelo nível de certificações técnicas muito elevado", como é o caso das certificações platinum da HPE, propartner da Veeam e Enterprise Solutions Provider da VMWare.

Estas certificações "foram herdadas da RIS 2048", fazendo agora parte das competências da nova empresa, explicou Patrícia David, acrescentando que estas parcerias permitem não só prestar serviços tecnológicos certificados, como disponibilizar níveis de descontos mais elevados que outros parceiros.

"Criar soluções para transformar ideias em sucessos" é o lema da empresa, refere Nuno Antunes Silva, senior technical consultant, ao Jornal Económico. "Os clientes acreditam na nossa capacidade de resposta e que queremos criar soluções", sublinha.

Em apenas quatro semanas, a empresa tem em negociação projectos no valor de quatro milhões de euros, com 10 clientes em projectos ativos. Durante o primeiro mês e meio de atividade, a Evonic apresentou um volume de negócios de três milhões de euros e Patrícia David antecipa que podem atingir os seis milhões de euros até ao final o ano.

> A diferenciação da nova empresa passa "pelo nível de certificações técnicas muito elevado"

Atualmente com três colaboradores, a Evonic está, neste momento, a recrutar consultores de tecnologia.

A RIS 2048 foi constituída no ano 2000 para agregar numa estrutura única a atividade de várias empresas de sistemas de informação que operavam na região Norte de Portugal. A empresa faturou 13 milhões de euros em 2016 e deverá atingir resultados consolidados (já incluindo a Evonic) de 18 milhões de euros, este ano. Tem, atualmente, cerca de uma centena de colaboradores.

As palavras-passe mais seguras

A 5 de maio comemora-se o Dia Mundial das Passwords. A gestão das palavras-passe pode ser complexo, mas é uma medida de segurança essencial. A Kaspersky Labs faz algumas recomendações sobre a matéria. Por exemplo, uma palavra-passe deve ter pelo menos oito carateres, incluindo maiúsculas, minúsculas, números e outros sinais. Datas de nascimento, nomes, combinações destes não são boas passwords. Também variantes como 123456 ou qwerty (seis teclas seguidas no teclado da maioria dos PC) devem ser esquecidas.

Pode criar uma "Story Algorithm". A Kaspersky exemplifica: "pense numa frase, letra de uma música, citação de um filme ou uma canção de infância; tire a primeira letra das primeiras cinco palavras; entre cada letra adicione um caracter especial". Assim terá uma password segura. Pode também utilizar mnemónicas e nunca deve partilhar as palavras-passe com ninguém, nem o método utilizado para a sua criação. A Kaspersky alerta "se um hacker descobrir um utilizador que se aproveita das letras das suas músicas preferidas para criar as palavras-passe, pode analisar o perfil do mesmo nas redes sociais e aceder à conta". Mesmo em casa, em computadores partilhados pela família, devem ser criadas contas distintas para cada pessoa. "Neste caso, não seria uma questão de confiança com a pessoa em causa mas o familiar pode ser persuadido a revelar a palavra-passe ou mesmo fazê-lo acidentalmente".

Usar a mesma palavra-chave em vários serviços pode ser perigoso. Basta ao hacker encontrar uma inofensiva para poder chegar à sua conta bancária ou portal da empresa. Memorize as passwords. Escrever a palavra passe no teclado várias vezes ajuda na memorização. Repita-o até que o processo seja automático. Em síntese, crie passwords seguras com base em símbolos e figuras com significado pessoal. Se precisar guardar em algum lado, opte por programas especiais de armazenamento de passwords.

DIREITO E TECNOLOGIA

Segurança nacional deve passar pela terra, mar, água e Internet

"Terá começado a guerra fria 2.0?", esta foi uma das hipóteses de base para o debate promovido pela PLMJ onde foi falado sobre um possível quarto ramo das forças armadas: a cibersegurança.

MAFALDA SIMÕES MONTEIRO
mmonteiro@jornaleconomico.pt

A sociedade de advogados PLMJ está a promover, durante o corrente ano, um ciclo de conferências intitulado "Direito Mega Wave" no qual serão debatidos vários temas relacionados com o direito e a tecnologia. As 10 conferências são coordenadas por Manuel Lopes Rocha, sócio coordenador da equipa de Propriedade Intelectual da PLMJ, e Pedro Lomba, consultor na PLMJ e estão a contribuir para o debate de ideias entre personalidades de ambos os meios: direito e tecnologia.

Na quarta sessão do ciclo de conferências, o tema central foi as "ameaças internas e a segurança nacional (e se a Rússia compra o Facebook?)". Os participantes cruzaram "saberes, experiências e informação" sobre estes temas.

"Terá começado a guerra fria 2.0?", esta foi uma das hipóteses de base para o debate que, entre outros temas procurou aferir as consequências da interferência de uma potência estrangeira nas eleições de um país soberano.

Manuel Lopes Rocha disse ao Jornal Económico que participaram nesta quarta sessão "dois dos melhores e mais informados especialistas na matéria": o coronel Luís Nunes e Jorge Portugal, diretor-geral da Cotec e que conta no seu currículo com o cargo de assessor do antigo Presidente da República. Segundo Lopes Rocha existe "uma convergência muito interessante nas preocupações e na esperança" quer por parte dos especialistas em tecnologias de informação quer nos juristas.

"Não existe apenas uma Internet negra, mas também um a Internet branca", assinala o advogado que está atento às questões de cibersegurança militar e civil e as perspetivas de futuro.

Durante a conferência, Luís Nunes referiu que na Alemanha já foi criado um novo ramo das formas armadas vocacionado para a ciberdefesa. O militar assinalou que é necessário investir, em seja qual for o modelo organizacional, em ciberorganização ou ciberdefesa. Luís Nunes destacou que apesar de já se verificarem muitas iniciativas em Portugal e de haver uma tomada de consciência sobre estas questões, tem de haver "organização e entrosamento" entre os vários atores. À semelhança do que já foi concretizado na Alemanha e, uma vez que a principal missão das Forças Armadas é a defesa, é "necessário haver investimento na segurança em terra, no mar, na água e também na Internet".

Foto cedida Plmj

Manuel Lopes Rocha, advogado da PLMJ

Na Alemanha já foi criado um novo ramo das formas armadas vocacionado para a ciberdefesa

Por seu lado, o responsável da Cotec, Jorge Portugal, apontou três grandes linhas de preocupação: em primeiro lugar assiste-se a um incremento sem precedentes da importância da Internet das Coisas. E exemplificou: um automóvel, e muitas outras "coisas", já têm uma série de equipamentos informáticos e uma potência extraordinária a que devemos estar atentos. Por outro lado, falou sobre a soberania nacional e sobre a soberania digital. No primeiro caso, o responsável sublinha o desafio que é a necessidade de proteção de dados com transparência, no segundo, os desafios são ainda maiores, uma vez que as novas realidades das redes sociais põem em causa os pilares da primeira.

No entanto, uma coisa é certa: o "nosso gémeo digital" existe e a "economia digital não vai voltar atrás".

Ciclo de conferências vai transformar-se em livro

Ao Jornal Económico, o advogado Manuel Lopes Rocha referiu que no final deste ciclo de conferências será publicado um livro com todas as intervenções. No corrente mês, o tema será a propriedade intelectual e direitos de autor que irá contar com a presença de quatro oradores que irão dissertar sobre infrações relacionadas com a propriedade intelectual: Miguel Guedes, advogado e compositor, Miguel Carreta, Tito Rendas, assistente da Faculdade Católica e Santos.

Cloud e inteligência artificial – sempre interrelacionados com o direito - serão os temas abordados em junho. Neste caso em particular Manuel Lopes Rocha mostra-se preocupado: "É extraordinário que ainda não se fala sobre a inteligência artificial", é necessário preparar o "estatuto jurídico dos robôs", porque "temos, pela primeira vez, máquinas que desenvolvem pensamento autónomo". São máquinas que vão "conseguir fazer as coisas com muito maior rapidez", o que representa "problemas de natureza organizativa e de substituição de pessoas", inclusivamente com qualificações. Estamos a falar de um "assunto de rotura civilizacional".

SERVIÇO DO GMAIL E DO WHATSAPP AFECTADOS

Esta semana, dois grandes serviços prestados na Internet foram afetados. Os utilizadores do serviço de correio eletrónico da Google foi alvo de um ataque de phishing que terá afetado 0,1% dos utilizadores e que foi "mitigado em menos de uma hora" segundo fonte oficial da Google Portugal.
Por seu lado o serviço de mensagens instantâneas WhatsApp, recentemente adquirido pelo Facebook, esteve em baixo um pouco por todo o mundo. A empresa não avança as causas para o sucedido referindo apenas que "utilizadores do WhatsApp em todo o mundo não conseguiram aceder ao WhatsApp por algumas horas. Já resolvemos o problema e pedimos desculpas pelos inconvenientes causados".
Relativamente ao Google, alguns utilizadores foram alvo de um ataque de phishing destinado a enganar os utilizadores induzindo-os a ceder os seus dados de acesso às contas de Gmail. Em resposta ao Jornal Económico, fonte oficial da empresa recomenda que "utilizadores que revejam as aplicações de terceiros ligadas às suas contas". A mensagem pedia ao recetor para abrir o que parecia ser um documento Google, que remetia para uma aplicação falsa que pedia os dados de acesso ao Gmail.
Fonte oficial da Google Portugal assinala que "tomámos medidas para proteger os utilizadores contra o spam que se fazia passar pelo Google Docs e que afetou menos de 0.1% dos utilizadores do Gmail".
A mesma fonte explica que "através de uma combinação de ações manuais e automáticas protegemos os nossos utilizadores, inclusivamente, removemos páginas e aplicações falsas". A empresa atualizou ainda os "mecanismos no Google Safe Browsing, Gmail e outros sistemas anti-abuso. Conseguimos parar esta ameaça em menos de uma hora". A Google recomenda aos utilizadores a revisão das aplicações de terceiros ligadas à sua conta Google, através do Google Security Checkup"

ENTREVISTA RODRIGO DÍAZ, chefe de laboratório de cibersegurança do departamento de investigação e inovação da Atos

Atos e parceiros investem 5,5 milhões em projeto de segurança IoT

O projeto, cofinanciado pela Comissão Europeia, visa o desenvolvimento de um selo dinâmico de segurança e privacidade, para mitigar as ameaças aos dispositivos e redes IoT.

MAFALDA SIMÕES MONTEIRO
mmonteiro@jornaleconomico.pt

O Advanced Networked Agents for Security and Trust Assessment in CPS/IoT Architectures (Anastacia) é um projeto financiado pela União Europeia que visa garantir a segurança dos sistemas cibernéticos (CPS) assentes na Internet das Coisas (IoT), através da criação de um selo dinâmico de segurança e privacidade.

O projeto é cofinanciado pela Comissão Europeia, através do programa Horizonte 2020, e visa "proporcionar uma solução integral para garantir a segurança e a confiança de serviços baseados na IoT que interagem por sua vez com recursos disponibilizados a partir da nuvem".

A iniciativa arrancou a 1 de janeiro de 2017 e terá uma duração de três anos. Representa um investimento de 5,5 mil milhões de euros, incluindo fundos provenientes do Horizonte 2020. Para além da Atos, integram este projeto 13 sócios de sete países diferentes (ver destaque).

O Anastacia irá "permitir a integração de mecanismos para a monitorização contínua dos dispositivos conectados, dando uma resposta automática aos ciberataques detetados". Até agora, "a insegurança neste ecossistema está relacionada com a falta de consenso na indústria e na Academia face à padronização de processos, protocolos e práticas para a disponibilização de serviços neste tipo de infraestruturas", explica a Atos. Rodrigo Díaz, chefe de laboratório de cibersegurança do departamento de investigação e inovação da Atos, explicou detalhes adicionais ao Jornal Económico.

Quais são os objetivos do projeto Anastacia?

O projeto Anastacia tem como objetivo fornecer um quadro seguro para a proteção de serviços e aplicações baseadas em Internet das Coisas (IoT). Este quadro inclui mecanismos para a configuração de políticas de segurança que devem ser cumpridas por uma plataforma IoT.

O Anastacia criará mecanismos para a aplicação de tais políticas de segurança, incluindo o monitoramento de dispositivos IoT, afim de detetar potenciais ameaças que possam implicar a violação da política de segurança.

O projeto Anastacia também desenvolverá capacidades de remediação e de criação de contramedidas para reagir a ameaças e ataques, mantendo o nível de segurança esperado para a plataforma IoT. Além disso, o nível de confiança da plataforma IoT poderá ser monitorado em tempo real com a criação do chamado "Selo Dinâmico de Segurança e Privacidade".

> "Espera-se que no início de 2018 os protótipos iniciais estarão disponíveis para mostrar as capacidades iniciais de deteção e remediação de ameaças contra eventos maliciosos", Rodrigo Díaz, Atos

Qual é o investimento global nesta iniciativa?

O Anastacia representa um investimento global de 5,5 milhões de euros. O investimento é distribuído pelos parceiros e pela comparticipação da Comissão Europeia, através do Horizonte 2020. A Atos participa com cerca de 10% do orçamento.

Quais serão os primeiros resultados visíveis deste projeto?

Ainda no primeiro semestre de 2017, o projeto produzirá a arquitetura global, com uma versão inicial das políticas de segurança a serem usadas e as potenciais ameaças a serem detetadas. Espera-se que no início de 2018 os protótipos iniciais estarão disponíveis para mostrar as capacidades iniciais de deteção e remediação de ameaças contra eventos maliciosos.

Qual o papel da Atos neste projeto?

A Atos lidera o projeto da arquitetura global do Anastacia e é responsável por projetar e implementar as componentes de monitorização e reação que irão permitir detetar ameaças, gerar eventos e alarmes e projetar contramedidas para prevenir as ameaças detetadas. Além disso, a Atos também é responsável por fornecer diretrizes para o desenvolvimento de software seguro de aplicações baseadas em IoT seguindo os princípios de segurança por design.

Quais serão os resultados do Anastacia?

O Anastacia poderá beneficiar em muitos aspetos diferentes empresas e cidadãos da Europa. Irá uma plataforma confiável para a disponibilização segura de serviços baseados em IoT, com deteção em tempo real de ameaças e a execução automática de contramedidas que mitiguem os efeitos nocivos de ataques potenciais.

Em conjunto, irão contribuir para aumentar a utilização e a aceitação de soluções IoT autónomas por parte dos utilizadores, que terá mais controlo sobre as mesmas através do "selo dinâmico de segurança e privacidade".

O Anastacia também alavancará o surgimento de novos serviços e aplicações baseadas em IoT, aumentando a oferta tecnológica de soluções IoT inovadoras, alavancando novos modelos de negócios emergentes que definitivamente suporão um impacto positivo no mercado português e europeu e sua economia.

Porque é preciso fazer investimentos avultados em segurança relacionada com a Internet das Coisas (IoT)?

Nos últimos seis ou sete anos, a Internet chegou a uma grande diversidade de novos dispositivos, para além dos computadores ou dos smartphones. Hoje temos televisões inteligentes que sincronizam todos os dispositivos em casa, dispositivos wearables que monitorizam a nossa atividade física, equipamentos domésticos que podem ser controlados remotamente, como a máquina de lavar, ou aplicações que permite gerir o consumo de energia em casa. Lâmpadas, veículos motorizados, interruptores, sensores de fumo, elevadores, semáforos, sapatos, óculos e muitas outras "coisas" estão ligados à Internet.

No entanto durante bastante tempo, o principal objetivo dos fabricantes de dispositivos estava concentrado nas funcionalidades que os novos dispositivos conectados poderiam ter, criando aplicações sem, no entanto, prestar atenção às medidas que deveriam ser tomadas para as proteger de ameaças de segurança.

Como resultado dessa negligência, hoje ocorrem ataques que assumem o controlo sobre os dispositivos conectados para executar ataques coordenados de negação de serviço (DDoS) que desativam importantes serviços de Internet ou

que alteram o comportamento normal de infraestruturas, incluindo críticas.
Além disso, aqueles dispositivos e aplicações conectados reúnem uma enorme quantidade de informações sensíveis que podem estar expostos a ataques maliciosos.

Quais são os métodos mais utilizados atualmente pelos atacantes para entrar nas redes e dispositivos IoT?
São duas práticas distintas que os atacantes exploram atualmente junto dos utilizadores de dispositivos IoT e redes associadas.
Por um lado, existem as chamadas práticas de "engenharia social" que os atacantes aproveitam para usar contra os utilizadores. Na prática, os hackers, vão procurar enganar-nos para assumir o controlo dos nossos dispositivos podendo levar-nos a instalar algum software mal-intencionado. Ao induzir-nos a instalar essas aplicações conseguem rastrear o nosso comportamento ou enviar arquivos ou senhas para destinatários mal-intencionados.
Os invasores podem também tirar partido da nossa negligência na configuração de dispositivos conectados. Um caso típico é a não-alteração da senha-padrão de acesso a redes Wi-Fi ou dispositivos IoT. Esta falha, facilita aos hackers o acesso aos nossos dispositivos e redes que podem, inclusivamente, assumir o controlo sobre todos esses dispositivos e redes. Depois de entrar, podem lançar ataques a alvos externos, sem serem detetados.
Uma outra prática, mais sofisticada está assente na exploração de vulnerabilidade de Dia Zero. Isto é, vulnerabilidades que ainda não são conhecidas nem foram identificadas pelos fornecedores de sistemas de segurança. Neste casos, as empresas e as pessoas estão mais expostas e vulneráveis. No entanto, manter o software e o firmware dos nossos dispositivos atualizados, com as versões mais recentes, é a melhor maneira de se proteger, reduzindo o risco de ser atacado.

PARTICIPANTES DO ANASTACIA

Archimede Solutions – Suíça;
Atos – França;
Device Gateway – Suíça;
Ericsson – Finlândia;
Mandat International – Suíça;
Montimage – França;
Conselho Nacional de Investigação Italiano (CNR) – Itália;
Universidade de Aalto – Finlândia;
Ubitech – Grécia;
Odin Solutions – Espanha;
Softeco – Itália;
Thales – França;
United Technologies Research Centre – Irlanda;
Universidade de Múrcia – Espanha;
Fonte: Atos

O desafio da regulamentação da proteção de dados

No dia 25 de maio de 2018 seremos confrontados com três tipos de Organizações. Organizações que não estarão em conformidade com o Regulamento, organizações em conformidade com o Regulamento e organizações que para além de estarem em conformidade com o Regulamento, irão conseguir demonstrá-lo através da apresentação de evidências e de práticas implementadas.

É fundamental que a metodologia usada pela organização coloque o seu enfoque e seja orientada para a implementação de práticas efetivas e que permita a análise e recolha de evidências. O Artigo 5º n.º 2 "O responsável pelo tratamento é responsável pelo cumprimento do disposto no n.º 1 e tem de poder comprová-lo («responsabilidade»)." e o Artigo 24 n.º 1 "o responsável pelo tratamento aplica as medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o presente regulamento." apontam o caminho correto a ser seguido.

O Regulamento é constituído por 99 artigos e 173 considerações, mas importa salientar que nem todos requerem a obtenção de evidências, sendo no entanto, necessário estarem acautelados seja por políticas seja por processos definidos na organização.

As organizações devem-se concentrar nas atividades que garantam a capacidade de uma rede ou de um sistema informático resistir a eventos acidentais ou a ações maliciosas ou ilícitas que comprometam a disponibilidade, a autenticidade, a integridade e a confidencialidade dos Dados Pessoais.

A nomeação do encarregado de proteção de dados (DPO), a elaboração da Política de Tratamento de Dados Pessoais, a criação de procedimentos que garantam a qualidade dos Dados Pessoais, a composição de comunicados de privacidade e a preparação de procedimentos de resposta aos pedidos dos Titulares do Dados estão entre as primeiras tarefas a serem realizadas.

As questões relacionadas com a privacidade dos Dados Pessoais devem ser incorporadas na sensibilização e formação de todas as equipas da organização sem exceção.

Deverão ser criados e implementados procedimentos de resposta aos novos direitos dos Titulares dos Dados, nomeadamente, o "direito de ser esquecido", o "direito ao apagamento", o "direito à portabilidade dos dados", o "direito à limitação do tratamento", o "direito de oposição", o "direito de retificação" e o "direito de acesso".

A entrada de novos sistemas e processos bem como todas as alterações significativas aos mesmos, devem ser realizadas tendo em conta os princípios da proteção de dados desde a conceção e por defeito, aplicando técnicas de pseudonimização e minimização dos Dados Pessoais entre outras.

O registo detalhado de todas as atividades de tratamento dos Dados Pessoais e a realização de avaliações de impacto sobre a proteção de dados (DPIA) são outras das atividades obrigatórias a fim de se cumprir o Regulamento.

Caso não disponha de recursos internos deve-se apoiar num parceiro que o possa acompanhar ao longo de todo o processo estratégico de implementação, eliminando o risco de incumprimento normativo, de eventuais coimas pela respetiva autoridade de controlo e sobretudo, eliminando o risco da ocorrência de algum tipo de incidente sobre os Dados Pessoais geridos na organização.

PROTEÇÃO DE DADOS

Regulamento dá mais poder aos titulares dos dados pessoais

Falta cerca de um ano para a entrada em vigor definitiva do novo RGPD. Os titulares dos dados pessoais vão ter uma palavra a dizer sobre quem pode e não pode ter a sua informação. As empresas têm de se preparar e encontrar um encarregado de dados. As coimas são avultadas.

MAFALDA SIMÕES MONTEIRO
mmonteiro@jornaleconomico.pt

O Regulamento Geral de Proteção de Dados vai entrar em vigor dentro de um ano. É uma matéria que implica quer com a privacidade dos dados dos utilizadores que passam a ter mais poder sobre os mesmos, mas reporta também a questões de segurança de todos e de cada um.

As multas são avultadas, podem chegar aos 20 milhões de euros, e os especialistas asseguram que serão aplicadas num primeiro momento, para servir de exemplo.

Atualmente em fase de transição, o Regulamento entrou em vigor no dia 25 de maio de 2016, nos termos do n.º 1 do seu artigo 99.º Estabelece o n.º 2 do mesmo artigo que o Regulamento "é aplicável a partir de 25 de maio de 2018, produzindo na mesma data efeitos a revogação da Diretiva n.º 95/46/CE)".

É por isso importante que as empresas se preparem para estar em conformidade com as novas regras europeias. Jane Kirkby, advogada e sócia da BAS Sociedade de Advogados, explica que "devemos considerar que há uma obrigação de adaptação aos aspetos e procedimentos que importam alteração para salvaguarda da aplicabilidade plena e do cumprimento do regulamento a partir de 25 de maio de 2018. A entrada em vigor dita que a sua implementação é devida desde essa data. Uma prática conforme o regulamento deve ser visada por todos os responsáveis pelo tratamento de dados pessoais e seus subcontratados e devem ser adotadas as medidas de adaptação que o próprio prevê".

Acresce que, "a partir do momento em que se tornar aplicável, o integral cumprimento do Regulamento é imediatamente suscetível de ser sindicado pelas autoridades de controlo. Ou seja, até lá, os responsáveis pelo tratamento dos dados devem desenvolver um complexo e exaustivo trabalho de preparação interna, que lhes garanta" dentro de um ano, "o tratamento dos dados por si realizado ou contratado é feito com total observância das novas regras aplicáveis em matéria de proteção de dados".

Jane Kirkby alerta que é "importante preparar desde já pois há um trabalho significativo a realizar" (ver artigo página VIII). "As empresas têm pouco mais de um ano para, por um lado, proceder a uma rigorosa avaliação da situação existente das bases de dados atuais de que dispõem e pelas quais sejam responsáveis e, por outro, definir quais os passos a seguir para gerar a conformidade da sua atividade com o novo enquadramento normativo e identificar que novos procedimentos ou medidas de segurança devem adotar para garantir o bom cumprimento do Regulamento".

O Regulamento Geral sobre a Proteção de Dados estabelece as regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Estará totalmente em vigor a partir de 25 de maio de 2018

Conformidade com RGPD e a segurança

Para que as empresas estejam em conformidade com a RGPD, devem desenvolver e rever, se necessário, os sistemas de informação de "acordo com caraterísticas concretas do tratamento dos dados, das medidas de segurança necessárias a garantir o cumprimento do Regulamento", defende Cláudia Monge, sócia da BAS Sociedade de Advogados. Para o efeito, "recomenda-se que tenham mecanismos de autenticação para entrada no sistema e para a execução de atos específicos e mecanismos de alerta para acessos indevidos ou intrusão (como log files ou traces files), que permitam a separação lógica de dados quando se justifiquem perfis de acesso diferentes e que sejam adotados processos internos para apreciar regularmente a eficácia das medidas técnicas de garantia da segurança do tratamento".

A conformidade com o regulamento é fundamental. Cláudia Monge sublinha que o "regulamento prevê expressamente que qualquer pessoa que sofra danos materiais ou imateriais devido a

Jane Kirkby, sócia da BAS Sociedade de Advogados

Cláudia Monge, sócia da BAS Sociedade de Advogados

O QUE É O RGPD?

O Regulamento Geral sobre a Proteção de Dados (aprovado pelo Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, a 27 de abril de 2016) estabelece as regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e revoga, com efeitos a partir de 25 de maio de 2018, a Diretiva 95/46/CE em transposição da qual foi aprovada a Lei portuguesa de Proteção de Dados Pessoais, (a Lei n.º 67/98, de 26 de outubro).

uma violação do RGPD tem direito a receber uma indemnização do pelos danos sofridos".

E as sanções são relevantes. "No caso de violação, intencional ou negligente, por parte do responsável pelo tratamento das obrigações que sobre si recaem nos termos do regulamento, pode ditar a aplicação de coima até 10 milhões de euros, ou, no caso de empresa, até 2% do seu volume de negócios anual a nível mundial. O limite máximo do montante da coima é elevado para 20 milhões de euros ou, no caso de empresa, 4% do seu volume de negócios anual a nível mundial, quando estejam em causa, designadamente, violações dos princípios básicos do tratamento, incluindo as condições do consentimento do titular dos dados". Neste caso concreto, os Estados-membros "podem estabelecer regras relativas a outras sanções aplicáveis em caso de violação do disposto no Regulamento", acrescenta Cláudia Monge.

As competências do CDO

O chief data officer, em português, encarregado da proteção de dados, é uma nova figura prevista pelo regulamento, em particular nas autoridades e organismos públicos.

Ao encarregado cabe "controlar da conformidade do tratamento com o regulamento". Este, explica Cláudia Monge, "é designado com base nas suas qualidades profissionais e, em especial, nos seus conhecimentos especializados no domínio do direito e das práticas de proteção de dados. Pode, em concreto, revelar-se adequado que seja um profissional de sistemas de informação, um jurista ou um médico para o tratamento de dados clínicos".

Cláudia Monge acrescenta que o regulamento "impõe a obrigação do responsável pelo tratamento e o subcontratante dotarem o encarregado de proteção de dados dos meios adequados ao desempenho das funções, pelo que a designação do encarregado com um determinado perfil não afasta que com este colaborem outros profissionais com perfis distintos que o auxiliem na execução das suas funções".

Kacper Pempel / Reuters

REGULAMENTO EUROPEU

Medidas para novas regras de proteção de dados

Comissão Nacional de Proteção de Dados anunciou uma lista de 10 medidas para preparar a aplicação do regulamento europeu de proteção de dados.

A Comissão Nacional de Proteção de Dados, que deverá ficar com algum tipo de responsabilidade como interlocutor dos detentores dos dados pessoais, embora ainda não esteja totalmente definida qual, publicou 10 medidas para preparar a aplicação do Regulamento Europeu de Proteção de Dados:

1 Informação aos titulares dos dados: deve rever a informação que fornece aos titulares dos dados, por escrito ou por telefone, no âmbito da recolha de dados, seja esta realizada diretamente junto do titular ou não.

2 Exercício dos direitos dos titulares dos dados: deve rever os procedimentos internos de garantia do exercício dos direitos dos titulares dos dados, atendendo a novas exigências específicas do regulamento neste domínio quanto à tramitação dos pedidos, em especial aos prazos máximos de resposta.

3 Consentimento dos titulares dos dados: deve verificar a forma e circunstâncias em que foi obtido o consentimento dos titulares, quando este serve de base legal para o tratamento de dados pessoais.

4 Dados sensíveis: deve avaliar a natureza dos tratamentos de dados efetuados, a fim de apurar quais os que se podem enquadrar no conceito de dados sensíveis, e consequentemente se aplicarem condições específicas para o seu tratamento, relativas à licitude do tratamento, aos direitos ou às decisões automatizadas

5 Documentação e Registo de atividades de tratamento: deve documentar de forma detalhada todas as atividades relacionadas com o tratamento de dados pessoais, tanto as que resultam diretamente da obrigação de manter um registo como as relativas a outros procedimentos internos, de modo a que a organização esteja apta a demonstrar o cumprimento de todas as obrigações decorrentes do RGPD.

6 Contratos de subcontratação: deve rever os contratos de subcontratação de serviços realizados no âmbito de tratamentos de dados pessoais para verificar se contêm todos os elementos exigidos pelo regulamento.

7 Encarregado de proteção de dados: deve preparar a designação do encarregado de proteção de dados com a antecedência devida, até porque este poderá desempenhar um papel fulcral neste período de transição para garantir que a organização cumpre todas as obrigações legais desde o início da aplicação do regulamento.

8 Medidas técnicas e organizativas e segurança do tratamento: deve rever as políticas e práticas da organização à luz das novas obrigações do regulamento, e adotar as medidas técnicas e organizativas adequadas e necessárias para assegurar e poder comprovar que todos os tratamentos de dados efetuados estão em conformidade com o RGPD a partir do momento da sua aplicação.

9 Proteção de dados desde a conceção e avaliação de impacto: deve avaliar rigorosamente o tipo de tratamentos de dados que tenha projetado realizar num futuro próximo, de modo a analisar a sua natureza e contexto e os potenciais riscos que possam comportar para os titulares dos dados, de modo a aplicar com eficácia os princípios da proteção de dados desde a conceção e por defeito.

10 Notificação de violações de segurança: deve adotar procedimentos internos e ao nível da subcontratação, se for o caso, para lidar com casos de violações de dados pessoais, designadamente na deteção, identificação e investigação das circunstâncias, medidas mitigadoras, circuitos da informação entre responsável e subcontratante, envolvimento do encarregado de proteção de dados e notificação à CNPD, atendendo aos prazos prescritos no regulamento.

BREVES

CNCP e PT juntam-se ao projeto "No More Ransom"

O Centro Nacional de Cibersegurança e Portugal Telecom acabam de se juntar à plataforma "No More Ransom", uma iniciativa conjunta da European Cybercrime Center (EC3) da Europol, da polícia holandesa, da Kaspersky Lab e da Intel Security que visa o combate ao ransomware. A plataforma No More Ransom (www.nomoreransom.org) foi criada há cerca de nove meses com o objetivo de incrementar o nível de cooperação entre as forças policiais e o setor privado com o objetivo de, em conjunto, combater a crescente ameaça do ransomware. A Polícia Judiciária já se tinha anteriormente associado à iniciativa.

Este tipo de malware bloqueia computadores e dispositivos móveis, cifrando os ficheiros e dados dos utilizadores. A plataforma visa mitigar os transtornos e prejuízos provocados pelo incremento deste tipo de ciberameaça.

Segundo a plataforma, só este ano, mais de 10 mil vítimas, a nível mundial, puderam desencriptar dispositivos afetados, sem pagar aos hackers, graças às ferramentas disponibilizadas gratuitamente no portal.

O projeto tem vindo a crescer e já conta com mais de sete dezenas de parceiros de todos os continentes, o que atesta a dimensão da ameaça. O site está disponível em 14 línguas e contém 39 ferramentas de decifragem que podem ser utilizadas de forma gratuita.

Roff lidera ranking

A ROFF, integrador de soluções SAP recentemente adquirida pela francesa Gfi, anunciou ter conquistado o primeiro lugar no ranking 2017 das melhores empresas trabalhar, com mais de 250 colaboradores, desenvolvido pelo Great Place to Work Institute A ROFF conta atualmente com cerca de 850 consultores e para além de Portugal conquistou igual reconhecimento no Brasil.

Loja da Huawei renovada

A loja da Huawei no Centro Comercial Colombo em Lisboa foi renovada no final do mês passado. A nova imagem, "reflecte a evolução da marca e da sua imagem", focada na fotografia móvel. A Huawei Consumer Business Group em parceria com a Phone House abriram a loja há um ano que é destacada pelo responsável da Huawei Consumer BG em Portugal, Michael Mao, como "uma experiência positiva" que se traduz no empenho da marca em estabelecer uma ligação mais forte e direta com os consumidores". O rebrandig será alargado a outros pontos de venda no retalho e a marca irá continuar a apostar no reforço da estratégia de ter espaços próprios e distintos nos pontos de venda, onde a empresa tem dado destaque especial aos novos equipamentos da gama P10.