DeviceLock® DLP

minitel NEXT

TECNOLOGIA DLP

UMA PEÇA CRÍTICA DO PUZZLE DA CONFORMIDADE

ÍNDICE

1 | O IMPACTO DA INOVAÇÃO TRAZIDA PELO GDPR

O GDPR, Regulamento Geral de Proteção de Dados, que entra em vigor a 25 de Maio de 2018 tem-se tornado num dos assuntos mais importantes para as empresas que tratam dados pessoais, devido às alterações significativas e ao risco legal associado.

Este novo regulamento relativo à proteção de pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação dos mesmos, revoga a Diretiva de Proteção de Dados (Directive 95/46/EC) e uniformiza os procedimentos e normas legais de proteção de dados para a EU.

O GDPR traz vários desafios às organizações que processam informações pessoais identificáveis (PII) dos seus clientes e funcionários.

O mais crítico são as enormes multas de não conformidade, que podem atingir até €20 milhões ou, no caso de um a empresa, 4% do volume de negócios anual, consoante o montante que for mais elevado, exigindo que as empresas estejam em conformidade com esta legislação. Por isso, este é um assunto debatido ao mais alto nível da administração das empresas. Para além disso, o regulamento prevê a obrigação de notificação da violação de dados, após terem conhecimento da mesma, à CNPD, num curto período de 72 horas que, se ultrapassado, pode significar elevadas multas para as empresas.

Outra alteração estratégica é que, pela primeira vez desde o princípio da "Privacy by Design" ou "data protection by design"(1), como é designado pelo GDPR, tornou-se uma norma legal na Europa. Para a maior parte das organizações, a conformidade com este princípio exige alterações estratégicas com a proteção de dados incorporada no desig, arquitetura de sistemas IT e práticas comerciais e, por isso, tem um impacto significativo a nível de custos de desenvolvimento e implementação. A disposição "data protection by design" é a mais importante e útil para que o GDPR possa, efetivamente, ser cumprido pelas organizações e a sua aplicação imposta pelas autoridades relevantes.

A terceira importante inovação é a extensão do âmbito das normas de proteção de dados da EU para todas as empresas estrangeiras que processem dados de residentes da EU.
Considerando estas e as outras inovações introduzidas pelo GDPR, não é surpresa que não só as empresas europeias, mas também de todo o mundo, que tratem dados pessoais de cidadãos europeus, estejam muito interessadas em perceber as obrigações desta lei e em desenvolver formas para alcançar a conformidade com o regulamento.

A questão da mais valia das tecnologias de DLP, na prevenção de fugas de dados, é primordial. Este documento responde a esta questão apresentando argumentos, explicações e conclusões que podem ser utilizados pelo CISO (responsável pela segurança da informação), donos de projetos, arquitetos de sistemas e designers, assim como outros especialistas, para formularem as suas próprias conclusões e compreenderem de que forma as funcionalidades DLP e as suas componentes podem ser utilizados nos projetos de adaptação dos sistemas IT, cumprindo o GDPR.

2 | A IMPORTÂNCIA DO DLP PARA A PRIVACIDADE E PROTEÇÃO DOS DADOS

Para analisar a importância das tecnologias DLP e alcançar, com sucesso, a conformidade com o GDPR, deve ser considerada a natureza do regulamento e os vários aspetos inter-relacionados com a sua aplicação prática. Estas considerações envolvem a dependência importante e fundamental entre segurança de dados e a informação sobre a proteção e privacidade, a interpretação do princípio de segurança de dados do GDPR, a compreensão de como o acesso e as operações de transferência de dados dos sistemas IT definem os requisitos chave do reforço de segurança e as tecnologias de segurança da informação que satisfazem estes requisitos.

2.1 | NÃO EXISTE PRIVACIDADE SEM SEGURANÇA

O GDPR tem como objetivo melhorar a privacidade da informação e a proteção nos sistemas de IT empresariais que processem dados pessoais de clientes e funcionários. Normalmente, estes problemas de privacidade específicos do IT estão relacionados com o crescente número de casos em que um sistema "concebido para alcançar objetivos benéficos, por exemplo, melhorar a eficácia da rede elétrica e aumentar a segurança, possam vir a afetar de forma adversa a privacidade dos indivíduos, à medida que processam informação sobre os mesmos (1)."

Alguns exemplos destes casos estão resumidos abaixo:

- Utilização de informação recolhida nas casas dos utilizadores através de contadores inteligentes da rede elétrica para revelar comportamentos dentro da própria casa;
- Perfis com dados pessoais identificáveis do comportamento do utilizador quando visita websites, para vender esta informação a agências de publicidade na Internet;
- Recolha de informação de pessoas privadas através de computadores ou vigilância da atividade na rede para fins não relacionados com a cibersegurança pública ou nacional.

Fundamentalmente, em todas estas violações à privacidade, existe um elemento em comum e intrínseco: são todas não intencionais, repercussões do tratamento de dados (1) – uma má utilização do acesso aos dados pessoais, que foi autorizado com propósitos legítimos. Desta forma, em todos estes casos a segurança (tratando-se precisamente de confidencialidade) dos dados tratados já tinha sido implementada, através da aplicação de medidas adequadas de controlo de acesso.

Isto significa que, por um lado, as violações à privacidade, devidas à má utilização dos dados, não podem ser evitadas exclusivamente com medidas de segurança, visto que estas têm como único objetivo autorizar ou negar o acesso aos dados pessoais, mas não detetar a finalidade do seu tratamento e controlar a capacidade do sistema as executar. De uma forma mais "inteligente" que o controlo de acesso, a proteção da privacidade dos processos empresarias sensíveis, para evitar a má utilização dos dados, tem de ser reforçada após a autorização de acesso aos dados pessoais.

Esta é a razão porque a obrigação das organizações de implementar medidas de proteção contra as ameaças decorrentes da má utilização dos dados pessoais está rigorosamente especificada no GDPR, através de um conjunto de princípios de tratamento de dados pré-estabelecidos (2), incluindo licitude, lealdade e transparência, limitação da finalidade, minimização dos dados, exatidão, limitação da conservação, storage, responsabilidade e integridade e confidencialidade.
Por outro lado, a própria aplicabilidade e importância em termos de proteção destas medidas de prevenção da má utilização dos dados, baseiam-se completamente na condição de que a confidencialidade dos dados já está assegurada. Consideremos os seguintes casos opostos:

- Se o acesso aos dados pessoais é controlado, pode ser concedido apenas aos componentes autorizados do sistema de tratamento que irão, posteriormente, evitar a má utilização dos dados nas suas próprias operações, enquanto que todas as outras – não autorizadas – entidades externas ou internas, não têm acesso aos dados pessoais, eliminado assim os riscos de violação da privacidade da informação.

- Em alternativa, se o acesso aos dados pessoais não é controlado, qualquer componente não autorizado do sistema e todas as entidades dentro e fora dele, por exemplo, funcionários maliciosos e hackers, podem aceder livremente aos dados e utilizá-los de forma indevida se pretenderem danificar a privacidade dos indivíduos cujos os dados são processados no sistema – independentemente da capacidade dos componentes do sistema autorizados para evitarem a utilização indevida nas suas operações.

Assim sendo, não pode existir privacidade sem segurança, uma vez que a falta de confidencialidade dos dados pessoais num sistema de tratamento torna a capacidade de prevenção da má utilização inútil.

O significado fundamental do reforço da segurança de dados para a privacidade da informação é totalmente reconhecido no GDPR, onde a definição específica de "integridade e confidencialidade", ou seja, dados tratados de forma a que garanta sua segurança, dedicada ao "trio CIA [3]", dos objetivos da info-segurança, foi adicionada aos princípios de proteção de dados do Artigo 5(1), que constituem os requisitos chave deste regulamento. Isto contrasta de forma positiva com a Diretiva 95/46/EC, onde o requisito relevante era especificado num parágrafo e artigo separado, dedicado meramente à segurança dos dados processados.

2.2 | DECIFRAR O PRINCÍPIO DA "INTEGRIDADE & CONFIDENCIALIDADE"

Embora o princípio da "integridade e confidencialidade" (posteriormente referido como o princípio I&C) abranja todos os propósitos da segurança da informação, incluindo confidencialidade, integridade e disponibilidade, uma análise simples da sua formulação e relações lógicas com os outros artigos e definições do GDPR, permite uma interpretação clara deste princípio relativamente ao problema da fuga de dados.

O princípio I&C exige que os dados sejam tratados de forma a que garanta a sua segurança, incluindo proteção contra o processamento não autorizado ou ilícito e contra a sua perda acidental ou destruição(2). O significado do termo "tratamento" pode ser encontrado no glossário do regulamento (artigo 4):

> **Tratamento** significa qualquer operação ou conjunto de operações executadas nos dados pessoais ou em conjuntos de dados pessoais, através de meios automatizados ou não, tais como (...), storage, (...) utilização, divulgação por transmissão, difusão ou de outra forma de disponibilização (2).

Como se pode verificar, tratamento indica vários tipos de operações incluindo, entre outras, as sublinhadas no texto: storage, utilização, divulgação por transmissão, difusão ou qulaquer outra forma de disponibilização de dados.

Na verdade, o princípio da I&C continua a ser aplicável e válido, não só para todos os tipos de operações de tratamento, mas também para os seus subconjuntos. Isto significa que a palavra "tratamento", na definição do princípio, pode ser substituída por qualquer sub-lista das suas operações de tratamento, incluindo as sublinhadas, sem quebra a validade do princípio. Fazendo esta substituição, obtemos um requisito totalmente consistente que é basicamente o princípio da I&C, mas se o relacionarmos com estas operações subjacentes, então do requisito resultaria o seguinte:

> **Os dados pessoais devem ser protegidos contra *armazenamento não autorizado ou ilícito, utilização, divulgação por transmissão ou qualquer outra forma de disponibilização e contra a perda acidental, destruição ou deterioração.***

Se compararmos este requisito com a definição de fugas de dados pessoais do glossário do regulamento no artigo 4, podemos ver que o texto em itálico no requisito acima indica uma violação de dados pessoais:

> **Violação de dados pessoais** significa uma falha de segurança que conduz à destruição acidental ou ilícita, perda, alteração ou divulgação não autorizada ou acesso dados pessoais transmitidos, armazenados ou processados de qualquer outra forma [2]."

Portanto, as palavras "violação de dados" podem ser utilizadas em vez do texto em itálico no requisito do I&C. Uma vez isto feito, a exigência transforma-se na articulação mais concisa da finalidade da segurança fundamental do GDPR: **os dados pessoais devem ser protegidos contra fugas de dados.**

Para finalizar a análise legal do texto, a definição de violação de dados no glossário do GDPR deve ser comparada com a definição de fugas de dados provenientes da indústria da TI :

Fuga de dados – um incidente de segurança no qual dados sensíveis, confidenciais ou protegidos são acidentalmente ou deliberadamente divulgados para um ambiente não confiável ou para utilizadores não autorizados, dentro ou fora da organização.

Através desta comparação, fica claro que a definição de fuga de dados do IT é um tipo específico de violação de dados, sendo que os outros tipos são destruição de dados, perdas (por exemplo, devido a falha de corrente) e alteração.

Resumindo esta análise, o GDPR, no seu princípio de I&C, juntamente com outros objetivos de proteção, exige que os dados pessoais **sejam protegidos contra fugas de dados.**

É também importante referir que, para além dos princípios da proteção de dados do artigo 5, a exigência de proteger os dados pessoais contra violações de dados e, consequentemente, fugas de dados está prevista no artigo 32 "Segurança no tratamento" do GDPR. O parágrafo 1 deste artigo prevê a implementação de medidas técnicas e organizativas para assegurar um nível de segurança adequado ao risco [2] para dados pessoais resultantes do seu tratamento, enquanto que o parágrafo 2 estipula especificamente que as violações de dados devem ser consideradas um risco sério para a segurança de dados pessoais:

> Para determinar o nível de segurança adequado deve ter-se em consideração o risco específico associado ao tratamento, em particular, de destruição acidental ou ilícita, perda, alteração, divulgação ou acesso não autorizado a dados pessoais transmitidos, armazenados ou de outra forma processados [2]."

2.3 | DO LEGAL AO TÉCNICO: TRANSPORTANDO O GDPR PARA O CAMPO DO IT

Declarado como neutro do ponto de vista tecnológico, o GDPR não define que tecnologias específicas devem ser usadas para implementar os princípios de proteção definidos. Contudo, fazendo o levantamento das especificidades do GDPR para o contexto do IT, onde, no fim de contas, as normas legais vão ter de ser aplicadas, é possível desenvolver um conjunto de requisitos técnicos que os componentes de segurança dos sistemas de tratamento de dados devem

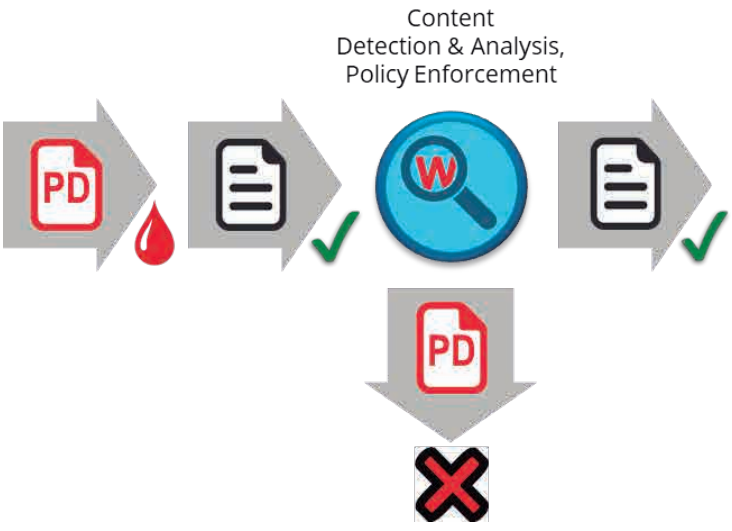
cumprir para proteger os dados contra fugas, de acordo com o regulamento.

O objetivo do GDPR é proteger um tipo específico de dados - dados pessoais, que contêm informação pessoalmente identificável (PII). As disposições do GDPR não são aplicáveis a dados que contenham outra informação que não PII.

Contudo, nos sistemas reais do IT que processam dados pessoais, são utilizados outros tipos de dados. Estes incluem informação de suporte às operações do negócio, comunicações dos funcionários, relatórios financeiros, estatísticas anónimas, etc. Estes tipos de dados não são pessoais, porque não contêm PII e, consequentemente, não é necessário que o seu tratamento esteja em conformidade com o GDPR. Por outras palavras, o tratamento de dados não-pessoais num sistema que cumpra o GDPR não dever ser (necessariamente) protegido ou restrito, embora o sistema deva proteger os dados pessoais.

Como consequência, em muitos casos, uma operação com dados, por exemplo, enviar um email, deve ser permitida porque não transmite dados pessoais e não viola o GDPR, mas a mesmíssima operação com dados pessoais deve ser proibida, porque leva à fuga de dados ou viola, de alguma forma, a privacidade – por exemplo, pode permitir aos controladores de dados identificar clientes para uma finalidades não aprovada pelos mesmos.

O ponto fundamental a anotar é que a única diferença a nível técnico entre estes dois casos, que de outra forma eram idênticos, é o conteúdo do dados tratados – PII ou não – e, consequentemente, a única forma de distinguir um caso do outro é analisar todo o conteúdo dos dados antes da saída dos mesmos.



Esta é a razão porque os componentes de segurança dos sistemas de tratamento em conformidade com o GDPR devem ser capazes, em primeiro lugar, de analisar o conteúdo dos dados processados face à política de proteção aplicada e, em segundo lugar, de aplicar as ações necessárias para prevenir perdas de dados – por exemplo, bloqueando uma operação com dados pessoais que violem a política de proteção.

É obrigatório que a análise e as ações de proteção sejam realizadas em tempo real, o que implica a sua execução automática. O objetivo é permitir que os componentes de segurança neguem atempadamente e eficazmente operações que violem as políticas, embora permitindo de forma transparente operações de dados executadas em conformidade no âmbito dos processos normais da empresa.

Por último, um requisito técnico também igualmente importante para os sistemas de tratamento, decorre do principio da I&C, exige que os dados sejam tratados de forma a que garanta a sua segurança em operações de tratamento, tais como storage, utilização, divulgação por transmissão e difusão. Assim sendo o sistema deve proteger os dados pessoais, incluindo dados em utilização, movimento e em descanso.

2.4 | O DLP É NECESSÁRIO PARA A CONFORMIDADE COM O GDPR

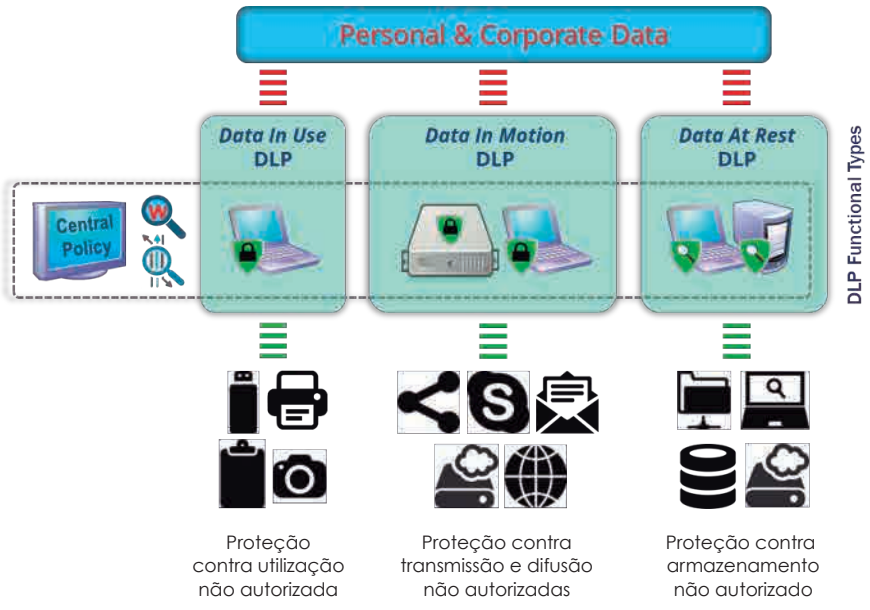
Que tecnologias existentes se enquadram nestes principais requisitos técnicos que decorrem do princípio da I&C do GDPR e que são essenciais para proteger os dados pessoais contra as fugas de dados: **análise do conteúdo em tempo real e aplicação de ações de proteção para vários tipos de dados em todos os seus estados (em utilização, em movimento e em descanso)?**

Uma avaliação de vários candidatos potenciais com base nestes critérios, revelou que a única tecnologia atualmente disponível que os satisfaz totalmente é a da prevenção de fugas de dados através conhecimento do conteúdo (DLP).

O que é o DLP?

O DLP é um sistema de tecnologias integradas que detetam e evitam a utilização não autorizada, transmissão e armazenamento de dados confidenciais, protegidos e sensíveis, aplicando uma combinação de métodos de análise contextual, de conteúdo e de aplicação de políticas de gestão de dados centralizadas.

Para a proteger os dados digitais nos três estados fundamentais, as soluções DLP implementam três tipos funcionais: "Dados em Utilização" (DIU), "Dados em Movimento" (DIM) e "Dados em Descanso" (DAR).



Dados em Utilização

O DLP controla o acesso a dados e operações de transferência em canais locais, periféricos e aplicações nos computadores endpoint, incluindo armazenamento fixo e amovível, teclado, impressão, screenshots, etc.

Dados em Movimento

O DLP previne fugas de dados através de comunicações de rede, por exemplo: email, webmail, Instant Messaging, social media, cloud-based e partilha de ficheiros P2P fi, HTTP/HTTPS, protocolos FTP/FTPS, SSL/TLS, etc.

Dados em Descanso

O DLP descobre conteúdo confidencial exposto em dados armazenados em ativos empresariais, tais como partilha de ficheiros e Network Attached Storage (NAS), sistema de ficheiros endpoint, bases de dados, repositórios de documentos e storage baseada na cloud. Se os dados não protegidos estiverem localizados no sito errado, DAR DLP pode iniciar automaticamente várias ações de remediação para evitar o acesso potencial não controlado, utilização e transmissão desses dados.

Diferentes tipos de DLP utilizam vários tipos de agentes de imposição. Só os agentes endpoint residentes podem ser usados para aplicar DLP em dados em utilização (DIU), embora os agentes endpoint, o hardware de rede residente e appliances de software virtuais possam complementar-se uns aos outros, para aplicar o DLP em os dados em movimento (DIM). Por sua vez, o DLP para dados em descanso (DAR), utiliza agentes endpoint (temporários ou residents) para fazer o scan de sistemas de ficheiros locais e os discovery servers residentes na rede também podem ser usados para fazer scaning remoto em partilhas de ficheiros, NAS, bases de dados, repositórios de documentos e storage cloud.

PORQUÊ O DLP E NÃO OUTRAS TECNOLOGIAS DE SEGURANÇA DA INFORMAÇÃO?

As capacidades funcionais das outras tecnologias avaliadas complementares ao DLP incluindo IRM – Information Rights Management e simples classificação de dados, não correspondem inteiramente aos critérios especificados. É importante ter em consideração que nem as tecnologias de IRM nem as de classificação de dados suportam originalmente a análise automática de conteúdo dos dados. Ambas delegam a tarefa da classificação do conteúdo aos utilizadores, como autores dos documentos ou aos administradores de segurança e poucas têm acesso a mecanismos de imposição. Vale a pena mencionar que, embora alguma classificação de dados moderna e sistemas baseados em IRM tenham começado a oferecer capacidade de análise de conteúdo automática, estas funcionalidades adicionais são atualmente implementadas através da integração das tecnologias DLP nos componentes do sistema.

Por outro lado as próprias capacidades do DLP cumprem todas os critérios. Quais são estas funcionalidades e vantagens do DLP?

A primeira e mais importante é a capacidade de analisar e classificar automaticamente o conteúdo da informação dos dados transmitidos, utilizados ou armazenados de vários tipos e formatos. Estes devem incluir não só ficheiros e emails, mas também mensagens instantâneas, posts para social media, webforms e webmails, dados em texto e em alguns cenários, mesmo metadata ou binários. No DLP, a análise de conteúdo é usada para detetar dados "confidenciais", "classificados" ou com conteúdo restrito idêntico e prevenir a sua utilização descontrolada, divulgação ou entrega a destinatários específicos, assim como o seu armazenamento em locais proibidos. Esta fusão de funcionalidades permite ao DLP cumprir os critérios chave de análise automática do conteúdo dos dados em todos os estados – utilização, movimento e descanso.

Diferentes tipos de DLP utilizam vários tipos de agentes de imposição. Só os agentes endpoint residentes podem ser usados para aplicar o DLP em dados em utilização (DIU), embora os agentes endpoint, o hardware de rede residente e appliances de software virtuais possam complementar-se uns aos outros, para aplicar o DLP em dados em movimento (DIM). Por sua vez, nos dados em descanso (DAR), o DLP utiliza agentes endpoint (temporários ou residentes) para fazer o scan de sistemas de ficheiros locais e os discovery severs residentes na rede também podem ser usados para fazer scaning remoto em partilhas de ficheiros, NAS, bases de dados, repositórios de documentos e storage cloud.

O segundo critério refere-se às ações de proteção em tempo real, novamente nos três estados que o DLP cumpre, através da capacidade de aplicar *controlos de segurança preventivos numa extensa gama de canais de fuga de dados e cenários*. Estes incluem praticamente todos os canais locais nos computadores endpoint, as comunicações de rede com maior risco, assim como vários dispositivos de armazenamento de dados, sistemas e repositórios.

Especificamente, os componentes do DLP podem aplicar um conjunto completo de ações de proteção como bloqueio, remediação, alerta, logue, shadow-copy e muitas mais.

Outra possibilidade essencial do DLP é o controlo de operações de dados baseadas no seu contexto, que é indispensável para prevenir a fuga de dados nos casos em que a deteção das violações à política de segurança não requeira análise de conteúdos, que pode ser muito exigente em termos de CPU e demorar muito a completar.

Uma vantagem substancial de utilizar controlos de DLP contextuais, é a simplicidade das políticas de DLP relevantes, a sua configuração e resolução de problemas. Para controlar as operações com dados, os principais sistemas de DLP suportam um conjunto abrangente de parâmetros contextuais, incluindo utilizadores, computadores e grupos, email de envio e recepção, identificação do utilizador (IDs) para mensagens instantâneas, tipo de portas locais e periféricos, números de série dos dispositivos juntamente com o fabricante, código de produto, direções para transferência de dados, dia/hora, portas de rede e endereços, etc. Existem dezenas destes parâmetros disponíveis nas políticas de DLP.

A última funcionalidade é o facto das políticas de DLP serem geridas centralmente pelos administradores de segurança e não pelos utilizadores ou administradores locais de sistemas.

O importante é que nos sistemas de DLP estas funções e funcionalidades estão profundamente integradas, tanto a nível de gestão como de execução. Esta integração também diferencia de forma única o DLP, comparativamente com outras tecnologias de segurança do IT, quando se trata de proteger sistemas contra fugas de dados.

Hoje em dia, não existe nenhum substituto real para o DLP para alcançar a conformidade com o GDPR. Por outras palavras, nenhuma outra tecnologia de segurança da informação tem o mesmo conjunto de capacidades funcionais optimizadas e dedicadas à finalidade de prevenção de fuga de dados pessoais ou quaisquer outros dados.

Uma evidência irrefutável é que muitas soluções de segurança IT utilizam o DLP como um add-on, um complemento para implementar funcionalidades de prevenção de fuga de dados nas suas áreas de competência específicas. Por exemplo, a indústria da segurança IT, está incluído nas plataformas de proteção endpoint (EPP); Em appliances UTM, email gateways e alguns sistemas de IRM e classificação de dados modernos. No campo do IT, as funcionalidades DLP estão muitas vezes integradas em sistemas de gestão avançada de email e gestão de documentos, serviços de partilha de ficheiros baseada em cloud e plataformas de SaaS – software as a service.

RESUMINDO

As tecnologias de DLP são indispensáveis para prevenir as fugas de dados pessoais nos sistemas de IT e por isso o DLP é necessário para implementar o princípio da "confidencialidade e integridade" e alcançar a conformidade com a regulamentação.

Na verdade, nem o DLP, nem qualquer outra tecnologia por si só, são uma bola mágica para o GDPR. Todo um puzzle de várias tecnologias complementares de privacidade e segurança da informação devem ser conjugadas para garantir a total conformidade com todas as disposições do regulamento.

Contudo, o DLP é a peça fundamental do puzzle da conformidade do GDPR.

3 | DATA PROTECTION BY DESIGN - A VIA PARA A CONFORMIDADE

3.1 | ENGINEERING INFORMATION PRIVACY

Indiscutivelmente a inovação mais significativa para os departamentos do IT empresarial que lidam com o GDPR, deriva do princípio de "data protection by design" - proteção de dados incorporada ao design, arquitetura dos sistemas de IT e práticas comerciais, introduzido no Artigo 25. Isto, juntamente com "a avaliação do impacto sobre a proteção de dados [1]" prevista no Artigo 35, essencialmente obriga à utilização **privacy engineering** pelas organizações, desenvolvendo ou reformulando os sistemas de IT de tratamento de dados pessoais para os tornarem conformes com o GDPR.

Especificamente, o Artigo 25(1) do GDPR estipula que:

> O controlador deverá, tanto na altura da *determinação dos meios de tratamento,* como no momento do tratamento, implementar as medidas técnicas e organizativas apropriadas… que foram concebidas para aplicar os princípios da proteção de dados... de forma eficaz e integradas as proteções necessárias no tratamento, de forma a satisfazer os requisitos deste regulamento e proteger os direitos dos data subjects [1]."

Esta norma legal de implementação de princípios de proteção de dados, juntamente com as funcionalidades da atividade da empresa, na fase de concepção do sistema de desenvolvimento, necessita categoricamente de capacidade de engenharia a nível da proteção dos dados pessoais – que é exatamente o objetivo da privacy engineering definida por NIST (National Institute of Standard and Technology)como disciplina especial dos sistemas de engenharia, centrada em libertar-se de condições que possam criar problemas para os indivíduos com consequências inaceitáveis, causadas pelo sistema de processamento de PII [2].

A funcionalidade fundamental da privacy engineering é que o seu modelo de risco é baseado na avaliação do impacto sobre a proteção de dados (AIPD). De acordo com o GDPR, as empresas são obrigadas à avaliação do impacto na proteção de dados (AIPD), definida como:

> Um processo concebido para descrever o tratamento, avaliar a sua necessidade e proporcionalidade e ajudar a gerir os riscos, direitos e liberdades naturais das pessoas, resultante do tratamento de dados pessoais, avaliando-os e determinando as medidas que respondem. Por outras palavras, o AIPD é o processo para *construir e demonstrar o cumprimento dos princípios do GDPR [4].*

O GDPR permite às organizações utilizar a metodologia do privacy engineering de avaliação do risco da privacidade, MITRE e NIST, provenientes dos standards internacionais ISO/IEC 27550.

Os Data Controllers e os Data Processors podem escolher qualquer processo sistemático ou a metodologia AIPD, "desde que considerem os componentes descritos no Artigo 35(7) [4]". Nas "Guidelines sobre o AIPD", estes requisitos são interpretados numa lista de critérios que devem ser usados para verificar se o AIPD é suficientemente bom para possibilitar a conformidade com o GDPR. Para além disso, estas diretrizes disponibilizam uma lista de metodologias AIPD já desenvolvidas em vários países da UE, assim com a referência ao standard ISO/IEC 29134:2017, dedicado às diretrizes de avaliação do impacto na privacidade.

Mudando o foco dos conceitos para um nível mais técnico, colocam-se três questões importantes para compreender a implementação da "data protection by design".

Colocam-se, então, as seguintes questões:

O QUE É QUE ESTE PRINCÍPIO REALMENTE SIGNIFICA PARA OS ARQUITETOS DE SISTEMAS?

Significa que, para além da principais funcionalidades que têm a ver com o negócio em si, a proteção de dados torna-se também outra funcionalidade de processamento muito importante. Deve ser concebida de raiz nos sistemas de tratamento, juntamente com as aplicações empresariais. Fundamentalmente, todo o sistema de tratamento estará pronto só depois das funcionalidades de proteção de dados terem sido implementadas e testadas com o mesmo nível de garantia de qualidade que as funcionalidades do sistema relacionadas com a atividade principal da empresa.

PARA QUE OPERAÇÕES DE TRATAMENTO É QUE UMA ANÁLISE DE IMPACTO DEVE SER FEITA?

De acordo com o Artigo 35(1), a AIPD deve ser executada em todas as operações de processamento que "possam muito provavelmente ter como consequência um risco elevado para os direitos e liberdades naturais das pessoas [1]" – isso acontece quando a divulgação, ou má utilização dos dados pessoais na operação, possa conduzir a danos significativo para os envolvidos. Para além disso, o Artigo 35(3) especifica, diretamente, três casos de atividades de tratamento em que deve ser feita AIPD, independentemente do nível de risco associado.

COMO SERÁ O PROCESSO DE INTEGRAÇÃO DE DADOS NA CONCEPÇÃO DO SISTEMA COM BASE NA AIPD?

Resumimos a sequência dos passos para este processo, no âmbito da fase de AIPD:

1. Uma operação de tratamento, ação ou atividade é avaliada relativamente aos tipos e nível de risco associados, incluindo tanto segurança de dados como riscos de má utilização dos dados.

2. Para cada uma das operações identificadas como de risco elevado, é identificado o seu tipo em termos de requisitos do GDPR, violados no caso de ocorrer uma situação de risco, por exemplo, princípios de proteção de dados, segurança no tratamento, etc.

3. As ferramentas de modelação de risco disponíveis na estrutura AIPD escolhida para o projeto são utilizadas para definir que finalidades da proteção dos dados (confidencialidade, integridade, disponibilidade, transparência) correspondem aos requisitos do GDPR afetados pela avaliação do risco.

4. As recomendações da AIPD são, finalmente, utilizadas para escolher a medida de proteção técnica e organizativa adequada e recomendada para eliminar ou reduzir o risco avaliado para um nível aceitável.

Seguem-se dois outros passos de engenharia à fase de AIPD, no ciclo de implementação e de proteção de dados no sistema:

5. É concebida uma solução para implementar as medidas escolhidas para neutralizar o risco.

6. Foram conduzidos uma série de testes para verificar que a solução implementada, (a) direciona os riscos para o grau necessário, b) não impacta negativamente as funcionalidades das aplicações do sistema e (c) o custo da sua implementação é aceitável, tendo em conta a probabilidade e a severidade do risco. Se a verificação falhar, a próxima iteração começa no passo 4 na fase de AIPD, seguida novamente por dois passos de engenharia, num ciclo, até ser concebida uma solução satisfatória ou o risco ser finalmente reconhecido como irremovível do contexto do sistema. No último caso, deve ser reportado à gestão dos projetos e ainda aprofundado em consulta com a Autoridade Relevante de Proteção de Dados (DPA).

De facto, englobar a cultura de desenvolvimento de no privacy engineering irá requer às organizações um maior investimento, esforço e tempo para que consigam ser bem sucedidas em desenvolvimentos e projetos futuros. Contudo, estes investimentos serão pagos através da poupança nos custos associados a fugas de dados, evitando multas por falta de conformidade com o GDPR - tudo graças aos seguintes benefícios fundamentais que a privacy engineering oferece às organizações:

- Permite implementar proteção de dados pessoais através de um método comprovado, previsível e repetitivo.
- Utilizando a privacy engineering na confidencialidade da informação, é possível alcançar e manter a conformidade com o GDPR.

- A privacy engineering torna os processos de implementação da proteção de dados e o alcance da conformidade totalmente coerentes. De facto, ambos são cumpridos com uma abordagem metódica e integrada e através de um único processo.

- Indispensável para a conformidade com o GDPR, a privacy engineering eleva a significância e a prioridade da proteção de dados para o nível da aplicação principal do negócio, e, como resultado, ajuda a garantir o orçamento e recursos necessários para esta tarefa.

3.2 | ESPECIFICIDADES DO 'DLP BY DESIGN'

Na concepção e arquitetura de uma solução de proteção de dados para analisar o risco do tratamento, o sucesso desta fase de engenharia e a qualificação a nível dos resultados depende substancialmente do rigor de como os fatores seguintes sejam considerados no processo de engenharia: a maturidade e disponibilidade das tecnologias de segurança da informação, adequadas para implementar as proteções necessárias, a finalidade do sistema de tratamento da empresa, a plataforma de aplicação, arquitetura e os tipos de componentes, assim como os perfis de ameaça específicos do sistema e os tipos de risco envolvidos.

Estas considerações são totalmente aplicáveis no caso das tecnologias DLP serem utilizadas num projeto, para neutralizar o risco de fugas de dados pessoais. A forma como são integradas na arquitetura e design dos sistemas de processamento é influenciada por vários fatores, sendo os mais importantes abaixo considerados:

OPÇÕES DE IMPLEMENTAÇÃO DO DLP

Hoje em dia, não só existem produtos DLP autónomos no mercado, como também são utilizados em vários tipos de soluções de segurança IT e serviços, como componentes complementares para a implementação de funcionalidades de prevenção de dados para domínios específicos de aplicação, alvo destas soluções.

Por exemplo, várias funcionalidades de DLP foram concebidas para plataformas de proteção endpoint (EPP), appliances de UTM, brokers de acesso a serviços cloud (CASB), gestão de direito de informação (IRM), soluções de classificação de dados, serviços de gestão de documentos e office suites, serviços de partilha de ficheiros cloud, firewalls de next generation e plataformas de software as a service (SaaS). Para além disso, alguns fornecedores de DLP disponibilizam códigos para integração de capacidades complementares em produtos dos clientes.

Assim sendo, quando as organizações precisam de tecnologias de DLP para responder ao risco de fugas de dados pessoais nos seus sistemas de tratamento, têm várias opções para implementar as funcionalidades de DLP, desde embeber o código DLP nas suas aplicações personalizadas, a utilizar capacidades DLP incluídas em suites de escritório, ou aplicações ou

plataformas de partilha de ficheiros que escolherem para o sistema, a utilizar funcionalidades DLP embebidas em appliances UTM ou CASB ou serviços e finalidades para utilizar produtos DLP stand-alone. Em cada caso particular, ao escolherem a melhor opção de DLP para implementar, devem ter em consideração os seguintes fatores:

- **A arquitetura de sistema escolhida e os tipos de componentes para a conformidade:** Infraestrutura e plataforma aplicacional (i.e. Google Cloud Platform, Microsoft Azure, etc.). Por exemplo, no caso de escolherem o Google Cloud, faz sentido considerarem os seus serviços DLP incluídos, acessíveis via APIs para implementação das proteções necessárias relacionadas com o DLP - desde que o âmbito de aplicação das funcionalidades seja suficiente.

- **Arquitetura escolhida e tipos de componentes do sistema a implementar, na lógica de aplicação empresarial.** No caso de a Microsoft Office Suite ter sido escolhida, por exemplo, para utilização no sistema como a suite de aplicações, os responsáveis pelo desenvolvimento dos sintemas devem verificar se as capacidades das funcionalidades de DLP integradas no Office são suficientes para implementar todas as funcionalidades de DLP requeridas pelo sistema, para prevenir ameças de fugas de dados pessoais.

- **Disponibilidade no mercado destes tipos de implementação de DLP, antecipados ou necessários para utilização na concepção do sistema de tratamento** – i.e. os códigos DLP SDKs de software, produtos DLP autónomos, várias soluções de segurança IT com funcionalidades de DLP incorporadas, etc.

- **O tempo e custo da integração, recursos e despesas, assim como o custo total de aquisição (TCO), devem ser avaliados** para todos os tipos de implementação de DLP potencialmente adequados para o projeto.

- Inicialmente, ao avaliar para escolher entre diversos produtos e serviços DLP disponíveis, deve ser verificado o aspeto funcional relativamente às necessidades do projeto, acompanhado por um comparativo das funcionalidades e caraterísticas de todos os produtos DLP qualificados, complementados e aferidos por uma análise comparativa do custo de aquisição TCO. Quando for realizado o comparativo das funcionalidades das diferentes alternativas de DLP, deve ser dada especial atenção aos seguintes critérios: tipos de DLP suportados (DLP de dados-em-utilização, DLP de dados em movimento e DLP de dados em descanso ou armazenados); espectro dos canais locais e de rede controlados; espectro de cenários de fuga bloqueados, qualidade dos controlos preventivos e ações corretivas; mecanismos de conhecimento de conteúdo suportados e controlos contextuais; escalabilidade da solução; integração da solução com os diretórios empresariais dominantes e, por fim, a sua resistência.

- Pode acontecer que nenhum dos produtos e soluções de DLP avaliados tenham, por si só, a abrangência funcional necessária, cobrindo todas as necessidades do projeto para prevenção de fuga de dados. Neste caso, fazer o bundle com soluções de DLP complementares cujas funcionalidades em conjunto sejam suficientes para o projeto, deve ser a opção. Por exemplo, construir um produto DLP endpoint e um serviço cloud de fornecedores diferentes.

O PRINCÍPIO DO MENOR PRIVILÉGIO NO CONTEXTO DO DLP

O princípio do menor privilégio é o paradigma lógico, nativo de gestão dos privilégios de acesso em todas as soluções de segurança de IT, que protegem a confidencialidade dos dados. A definição original deste principio estipula que qualquer programa e qualquer utilizador do sistema devem funcionar utilizando o conjunto de privilégios minimo e necessário para completar a tarefa. Basicamente, este princípio limita o dano que pode resultar de um acidente ou erro [5].

Aplicando este princípio às soluções de DLP, os administradores de segurança podem atribuir direitos de utilizador às funções e tarefas relativas à transferência, recepção e armazenamento de dados. O ambiente seguro que daí resulta, permite que as ações de todos os utilizadores legítimos prossigam sem impedimentos, enquanto que as tentativas inadvertidas ou deliberadas de realizar operações fora dos parâmetros definidos são bloqueadas.

Para utilizar a técnica do menor privilégio e configurar as políticas de DLP da forma mais optimizada, devem ser tomadas em consideração certas especificidades dos mecanismos preventivos de DLP. Existem dois tipos de considerações: inspeção a nível do conhecimento do conteúdo, executando a análise de conteúdo, classificação de dados e controlos contextuais que detetam a utilização de vários parâmetros do contexto da operação, de forma a decidir se a operação é permitida ou se deve ser evitada.

Por exemplo, estes parâmetros incluem quem (o utilizador) ou o que (o processo) inicia esta operação, quando, de onde e para onde ou para quem e como – através de que canal ou dispositivo - os dados são utilizados ou transferidos. Tanto os mecanismos contextuais, como de conhecimento de conteúdo podem ser utilizados numa única politica de DLP, implementando a princípio do menor privilégio na medida do possível.

As especificidades de optimização da aplicação do DLP são um misto tanto dos controlos contextuais, como os métodos de inspeção de conteúdo e devem ser utilizadas só em regras para estes cenários de fuga, onde a decisão de permitir ou bloquear depende exclusivamente do conteúdo desses dados.

Ao mesmo tempo, em todos estes cenários onde a análise das operações dos parâmetros contextuais é suficiente para detetar violações à politica de segurança, só os controlos contextuais devem ser utilizados logicamente nas regras DLP relevantes, sem envolver a análise de conteúdo desnecessária, que pode ser muito intensiva em termos de CPU e demorar muito tempo a finalizar. Outra vantagem substancial de utilizar os controlos de contexto do DLP sempre que possível, é a simplicidade das políticas DLP relevantes, a sua configuração e a resolução dos problemas. Para além disso, os controlos contextuais não têm a advertência de falsos positivos, que afetam a precisão e utilidade de muitos dos métodos de análise de conteúdo.

Os sistemas de DLP modernos podem reforçar os controlos preventivos numa multitude de parâmetros contextuais, incluindo utilizadores, computadores e os seus grupos, endereço de emails de expedidores e receptores, identificadores do utilizador (IDs) para mensagem instantânea, tipos de portas locais e periféricos, números de série dos dispositivos em combinação com os ID dos produtos e fornecedor, direções do fluxo de transferência de dados, aplicações de rede ou protocolos utilizados para a operação, portas de rede e moradas, se o storage media está encriptado ou a comunicação está protegida - SSL, data e tempo da operação, etc. - podem existir dezenas de parâmetros para utilização nas políticas de DLP.

A utilização de controlos contextuais de DLP tem provado ser altamente eficaz nas operações internas das empresas onde, tipicamente, podem ser controlados muitos cenários de fuga de dados sem analise de conteúdo.

UTILIZAÇÃO DO DLP PARA ALÉM DA SEGURANÇA DE DADOS

O conjunto de funcionalidades de segurança específicas das tecnologias DLP faz com que possam ser utilizadas, não só para aplicar o princípio do I&C, mas também para implementar proteções para outros princípios de privacidade adotados no Artigo 5 do regulamento.

Especificamente, a possibilidade do DLP efetuar a recolha de registos extensivos para auditoria sobre as ações relacionadas com acesso aos dados, armazenamento e operações de transferência utilizadas, para facilitar o princípio da "transparência" o que, de acordo com o artigo 39 do GDPR, requer que qualquer informação ou comunicação relacionada com o tratamento desses mesmos dados pessoais possa estar facilmente acessível e compreensível, para poder ser utilizada uma linguagem simples e clara [1].

Outra funcionalidade do DLP - descoberta de conteúdos dos dados armazenados nos ativos empresariais - pode ser utilizada para reforçar o princípio de "limitação do storage", que requer que os períodos de storage dos dados pessoais sejam limitados ao momento em que são tratados licitamente. Os componentes do DLP fazem a análise do conteúdo dos dados residentes nos computadores endpoint, partilha de ficheiros, NAS, repositórios de documentos em redes empresariais, assim como dados guardados em storage cloud autorizada. Os dados pessoais com períodos de storage expirados sejam localizados pelo scan, os componentes de DLP podem protegê-los com ações de correção automática e podem iniciar processos de gestão de incidentes com alertas em tempo real, enviados para sistemas SIEM e/ou enviados por email para os funcionários responsáveis da segurança na organização.

FOCO NA PREVENÇÃO DAS FUGAS DE DADOS INTERNAS

Essencialmente, o GDPR tem como objetivo proteger os dados pessoais de dois tipos de ameaças internas, originadas dentro das organizações, que utilizam estes dados nos seus processos de negócio. O primeiro tipo relaciona-se com a violação das informações de privacidade

resultantes de uma má utilização dos dados pessoais, derivadas de acessos autorizados licitamente, para finalidades de tratamento. O segundo tipo são as fugas de dados que resultam de acessos não autorizados à informação pessoal, por indivíduos dentro da empresa – utilizadores legítimos dos sistemas IT.

Esta é a razão porque, ao avaliar as várias opções de DLP para implementar proteções confidenciais contra fugas de dados pessoais, os designers do sistemas devem dar prioridade às soluções DLP focadas na prevenção de fugas de dados internas como a forma mais eficaz de alcançar a conformidade como GDPR.

Uma funcionalidade diferenciadora destas soluções é a possibilidade de melhorar as capacidades funcionais dos agentes endpoint DLP para evitar não só as fugas de dados através de canais locais de endpoint (DLP de dados em utilização) e transmissões de dados não autorizadas através das comunicações de rede (DLP de dados em movimento), assim como suporte à descoberta de conteúdo em sistemas de ficheiros locais e partilha de redes acessíveis (DLP para dados em descanso).

Uma das soluções de DLP que suporta totalmente estas capacidades é o **DeviceLock DLP**, cujo objetivo é a prevenção de fugas de dados através de computadores endpoint empresariais.

4 | O DEVICELOCK DLP PARA PARAR AS FUGAS DE DADOS NA ORIGEM

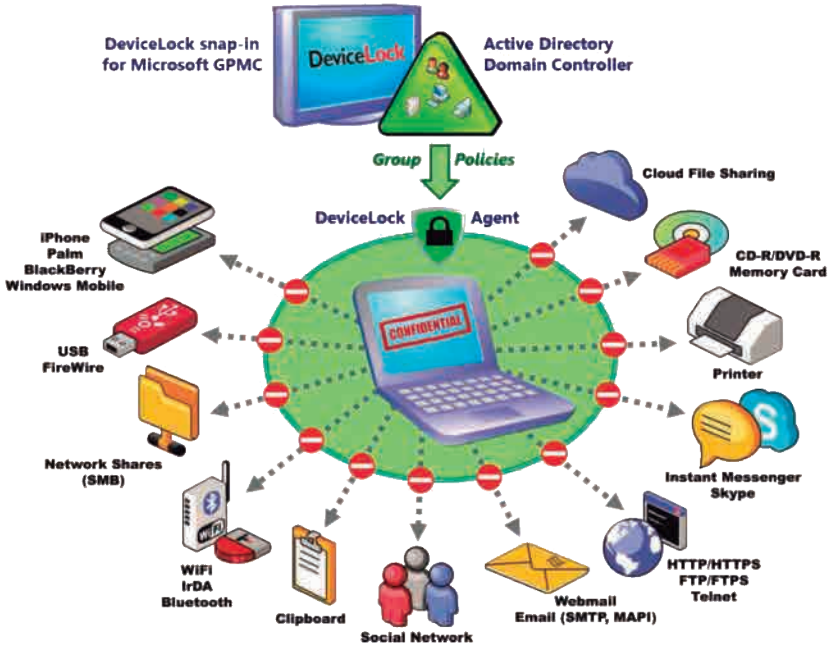
Para qualquer empresa no panorama da economia moderna, a informação utilizada nos sistemas de IT empresariais na forma de dados digitais tornou-se um ativo intangível fundamental para o seu crescimento, sustentabilidade e competitividade. Esta informação inclui a propriedade intelectual, os dados dos clientes, dados financeiros da empresa e segredos de negócio, PII e PHI de clientes e funcionários, know-how tecnológico, inteligência competitiva e outros tipos de conhecimento relevante. Os dados são o coração do IT da empresa e, tal como uma perda de sangue é altamente perigosa para os organismos vivos, o mesmo se passa com as fugas de dados nas empresas.

Proteger os dados é fundamental na nossa realidade hiper-ligada, onde as comunicações de dados móveis, a Internet, social media, email e outras aplicações de consumo são omnipresentes, assim como a comercialização do cibercrime. Tudo isto aumenta substancialmente as ameaças de segurança IT. A pandemia global de fugas de dados resultantes do acesso não autorizado a difusão de informação empresarial valiosa pode conduzir a perdas financeiras enormes, desde litigação com elevados custos, multas por compliance aplicadas pelas autoridades, danos à reputação e perda de receitas.

É especialmente perigoso que a maior parte dos incidentes de fugas de dados esteja relacionados com fontes internas, utilizadores normais dos sistemas IT das empresas, como colaboradores,

fornecedores e clientes. A primeira razão é de natureza humana – as pessoas cometem erros acidentais e podem ser negligentes no manuseamento dos dados. Por outro lado, pode existe uma má conduta intencional. Muitos são vitimas de ataques de social engineering, tais como email ou social media phishing.

O **DeviceLock DLP** foi concebido para resolver os problemas das fugas de dados internas. É uma solução de software para as organizações que precisam de uma abordagem simples e com um custo acessível, para a prevenção de fugas de dados de portáteis Windows e Mac, computadores desktop, sessões virtualizadas Windows e aplicações. O **DeviceLock DLP** implementa e coordena eficazmente um conjunto completo de controlos de contexto e de reconhecimento do conteúdo dos dados-em-utilização, dados-em-movimento e dados-em-descanso, desenvolvido especificamente para prevenir fugas de informações nos endpoints empresariais.



DeviceLock DLP recorre a um agente de execução muito leve que é instalado em todos os computadores protegidos com uma Política de Grupo centralizada que pode ser ajustada a qualquer dimensão e tipo de rede empresarial. Existem também consolas centrais tradicionais que podem ser usadas para gerir Macs, ambientes que não sejam AD LDAP e/ou grupos de trabalho Windows. Correndo de forma transparente para os utilizadores e aplicações na esfera de ação das aplicações internas correntes nos processos de negócio, os **Agentes do DeviceLock** detetam e evitam o acesso não autorizado aos dados e operações de transferência nos computadores protegidos.

A inspeção multicamada e o motor de intercepção disponibilizam, a nível contextual, um controlo granular sobre os vários trajetos de uma fuga de dados. Para uma garantia ainda maior de que nenhuns dados sensíveis escapam, podem ser aplicados uma análise de conteúdo e filtro às transferências e partilhas de dados nos endpoints com removable media, impressoras

E dispositivos Plug-n-Play (PnP), assim como protocolos de rede associados à ligação de serviços e aplicações à Internet.

Para além disso, podem ser utilizados o **Servidor Discovery do DeviceLock** e os **Agentes Discovery do DeviceLock** para examinar e encontrar documentos em descanso, verificar se existe qualquer conteúdo armazenado exposto e sensível em sítios proibidos nas partilhas de rede, sistemas de armazenamento e computadores endpoint Windows dentro da rede empresarial. O DeviceLock Discovery oferece opções para proteger contra estas fugas de dados potenciais, com ações de correção automática e procedimentos de gestão de incidentes, com alertas em tempo real enviados para os sistemas e/ou email dos responsáveis pela segurança dos sistemas na organização

Com o **DeviceLock DLP,** os administradores de segurança podem atribuir direitos em função do cargo do colaborador, relativamente à transferência, recepção e armazenamento de dados em computadores empresariais. O ambiente seguro daí decorrente permite que as ações dos utilizadores legítimos prossigam desimpedidas e que as tentativas inadvertidas ou deliberadas de realizar operações fora das regras estabelecidas sejam bloqueadas.

A solução do **DeviceLock DLP** é simples, fácil de utilizar e concebida para se adaptar sem esforço tanto a pequenas, como grandes instalações, simplificando a implementação e gestão do DLP, de forma a que seja quase sempre executado pelos administradores internos do Windows, utilizando a consola de Gestão do Active Directory's Group Policy da Microsoft ou as consolas complementares do DeviceLock. O pacote completo oferece um nível de funcionalidades sem precedentes, comparativamente às soluções DLP endpoint, com um nível de preço acessível.

Por prevenir as fugas de dados nos endpoint eficazmente, o **DeviceLock DLP** ajuda as organizações a minimizar os riscos de segurança relacionados com a segurança da informação e a alcançar a conformidade com as políticas de utilização de dados empresariais, standards de segurança IT e a legislação de proteção de dados.

5 | CONCLUSÃO

Embora o GDPR ainda não esteja a ser aplicado, o primeiro resultado já está em cima da mesa – do conselho de administração das empresas: as enormíssimas multas escalaram do tópico da proteção da privacidade da informação para o nível da gestão executiva, tornando-se assim o assunto top do ano em todo o mundo. Contudo, o GDPR não só promove forçosamente a cultura do privacy engineering do IT empresarial, adotando o princípio do "data protection by design", como também disponibiliza à organização um ecossistema completo de ferramentas, métodos, documentos legislativos e autorizações necessárias para implementar esta cultura em todos os procedimentos reais do IT.

Para que o desenvolvimento abranja o privacy engineering, as organizações têm de ser capazes de implementar a proteção de dados pessoais através de um método comprovado, controlado, previsível e repetível. O privacy engineering poderá garantir o cumprimento pleno dos processos de implementação da proteção de dados para alcançar a conformidade com o GDPR. Para além disso, a abordagem do privacy engineering elevará a prioridade do desenvolvimento da proteção de dados aplicando-o às atividades fundamentais da empresa e, por sua vez, contribuirá com os recursos e orçamento necessários.

Sendo neutro do ponto de vista tecnológico o GDPR, não recomenda quaisquer tecnologias de proteção de informação. Todavia, como tem por objectivo proteger dados de um tipo de conteúdo específico – informação pessoalmente identificável (PII), a implementação do princípio do GDPR da "integridade e confidencialidade requer que a análise de conteúdo e a aplicação das ações de proteção para prevenir a fuga de dados pessoais, em todos os seus estádios, sejam executadas em tempo real: em utilização, movimento e descanso. Atualmente, as tecnologias DLP são as únicas que suportam totalmente estas funcionalidades – consequentemente, o **DLP é necessário para implementar o princípio da "integridade e confidencialidade" e alcançar a conformidade com o GDPR.**

Sendo neutro do ponto de vista tecnológico o GDPR, não recomenda quaisquer tecnologias de proteção de informação. Todavia, como tem por objectivo proteger dados de um tipo de conteúdo específico – informação pessoalmente identificável (PII), a implementação do princípio do GDPR da "integridade e confidencialidade requer que a análise de conteúdo e a aplicação das ações de proteção para prevenir a fuga de dados pessoais, em todos os seus estádios, sejam executadas em tempo real: em utilização, movimento e descanso. Atualmente, as tecnologias DLP são as únicas que suportam totalmente estas funcionalidades – consequentemente, o DLP é necessário para implementar o princípio da "integridade e confidencialidade" e alcançar a conformidade com o GDPR.

Outro facto de extrema importância, é que o objetivo do GDPR é a proteção de dados pessoais, principalmente contra ameaças internas, com origem no próprio sistema interno de

processamento de dados – má utilização de dados que leva a violações da privacidade da informação ou acesso interno não autorizado à informação pessoal que provoca a fugas de dados. Esta é a razão porque as soluções mais eficazes para implementar proteções à confidencialidade, contra fugas de dados pessoais são os módulos DLP enfocados em prevenir fugas de

Vale também a pena mencionar que, para além da proteção da confidencialidade, a conjugação única de funcionalidades específicas do DLP torna-as vitais na implementação de proteções relativamente a outros princípios de privacidade de dados do GDPR - especificamente os princípios de "transparência" e "limitação de "storage".

Como nota final, de forma nenhuma este argumentos a favor do DLP e conclusões pretendem menosprezar o papel e a importância de outras tecnologias de proteção de dados e soluções para alcançar a conformidade com o GDPR.

Nem o DLP, nem qualquer outra tecnologia específica, só por si, pode funcionar como "bola de cristal" para o GDPR. É necessário um puzzle de várias tecnologias que melhoram a segurança da informação e privacidade, conjugadas para garantir a conformidade total com as disposições deste regulamento. Porém, o DLP é uma peça fundamental no puzzle de conformidade com o GDPR.

6 | REFERÊNCIAS

[1] Council of the European Union, European Parliament, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC," Official Journal of the European Union, vol. L119, pp. 1-88, 4 May 2016.

[2] S. W. Brooks, M. E. Garcia, N. B. Lefkovitz, S. Lightman and E. M. Nadeau, "NISTIR 8062, An Introduction to Privacy Engineering and Risk Management in Federal Systems," NIST, Gaithersburg, 2017.

[3] Wikipedia, "Information Security," Wikimedia Foundation, 20 February 2018. [Online]. Available: https://en.wikipedia.org/wiki/Information_security. [Accessed 21 February 2018].

[4] Article 29 Data Protection Working Party, "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679," WP 248 rev.01, European Commission, Brussels, 4 Oct 2017.

[5] J. Saltzer and M. Schroeder, "The Protection of Information in Computer Systems," in Fourth ACM Symposium on Operating System Principles, Yorktown Heights, Oct 1973.