Como Manter um Segredo... Secreto

Bernardo Patrão

Engenheiro Sénior da Critical Software. É licenciado em Engenharia Informática, pela Universidade de Coimbra. Iniciou a sua colaboração com a Critical Software aquando do seu estágio no verão de 2002, focando-se em sistemas confiáveis e sistemas operativos de tempo real, mudando-se posteriormente para a área de Segurança da empresa. Participou em vários projetos de desenvolvimento de software e auditoria na área de Segurança de Informação, sendo certificado em ISO 27001. É atualmente Gestor Técnico da solução csSECURE.

Resumo

A fuga de informação é um problema acidental? A necessidade de proteção da informação nas organizações está presente na mente de qualquer profissional de segurança. Acontecimentos recentes (WikiLeaks, fugas de dados pessoais de clientes, etc.) mostram-nos que a informação confidencial não está segura na sua forma tradicional, e o acesso à informação não é, de todo, controlado.

As ferramentas de segurança mais usadas atualmente são sobretudo centradas na rede e/ou no computador, protegendo a informação de ataques externos (hacks, vírus, cavalos de Tróia), mas não protegem as organizações contra fugas de informação. As técnicas mais promissoras para controlar as fugas de informação são o ERM (Enterprise Rights Management) e o DLP (Data Loss Prevention).

Os inconvenientes das soluções de ERM (dependência do utilizador, falta de classificação automática e a complexidade de administração) são colmatados com os pontos fortes dos produtos DLP, resultando numa abordagem inovadora no campo da segurança da informação.

Há soluções que combinam o ERM e o DLP, baseadas no conceito de segurança multinível que efetivamente protege as organizações contra fugas de informação, mantendo o controlo sobre os dados corporativos e monitorizando as ações dos utilizadores sobre a informação produzida.

Abstract
How to Keep a Secret… Secret

Is information leakage an accidental problem? The need for information protection within organisations, is present in the mind of every security professional. Recent history (WikiLeaks, information leakage of personal client data, etc.) teaches us that confidential information is not secure in its traditional form and access to information is not controlled at all.

Common security tools in place are typically network and/or computer centric, protecting information from external attacks (hacking, virus, trojans, etc.) but fail to secure companies against information leakage. The most promising techniques for controlling information leakage are ERM (Enterprise Rights Management) and DLP (Data Loss Prevention).

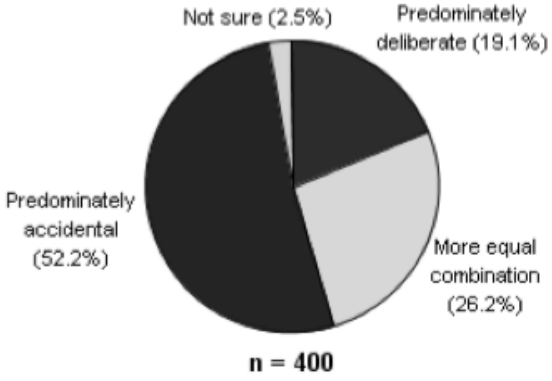
The drawbacks of the ERM solutions (user dependency, lack of automatic classification and administration complexity) and the strengths of DLP products combined, would reap the benefits of ERM and DLP, resulting in an innovative approach within the information security field.

There are solutions that combine ERM and DLP solution, based on the Multilevel security concept that effectively protects your organization against information leakage, while maintaining control over corporate data.

As fugas de informação são um problema real e cada vez mais comum. Quase todos os meses, notícias sobre fugas de informação numa organização tornam-se públicas. No entanto, estes são os casos conhecidos do público em geral e que têm um impacto mais visível nas organizações. Milhares de fugas de informação de organizações acontecem todos os dias, e maioritariamente por acidente, displicência ou mesmo com intenção!

De acordo com estudos recentes, a vasta maioria das fugas de informação têm uma natureza acidental: "O IDC[1] acredita que a maior parte das fugas de informação vão continuar a ser acidentais, mas esperamos um número crescente de ataques cuidadosamente planeados por sofisticadas organizações criminosas. Também acreditamos que os impactos financeiros dos incidentes deliberados de perdas de informação são normalmente muito maiores que os acidentais." (IDC, 2010).

Figura 1 – Distribuição de incidentes relacionados com segurança de informação



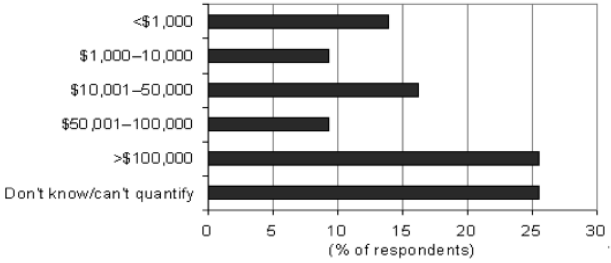
Fonte: International Data Corporation (IDC, 2010). Disponível em http://www.idc.com.

Isto significa que as fugas de informação não são apenas o resultado de atos intencionais, mas também de ações sem intenção que os colaboradores da organização podem executar. As fugas de informação acidentais são talvez as mais perigosas, pois o utilizador não está consciente (pelo menos no imediato), nada fazendo para que tal não ocorra.

1 International Data Corporation.

Além de serem um problema real, as perdas de informação podem representar um custo muito elevado para as organizações. De acordo com o estudo Information Protection and Control (IDC, 2010), 26% das empresas refere que eventos de perdas de informação tiveram um custo superior a $100.000!

Figura 2 – Custo de perdas de informação



Fonte: International Data Corporation (IDC, 2010). Disponível em http://www.idc.com.

A perda de informação tem um custo direto (Kolodgy, 2011): a propriedade intelectual ou a informação industrial perdida na fuga, assim como a gestão das consequências desta. Tem também um conjunto de custos indiretos[2], como: perda de credibilidade no mercado, perda de propriedade intelectual que pode levar à erosão de vantagens competitivas, e a falha de cumprimento com determinada legislação.

Definição do Problema

Hoje em dia pouca ou nenhuma informação em papel está envolvida nos processos centrais das organizações. A informação crítica de negócio está cada vez mais no formato digital. Estudos recentes mostram que a tendência de crescimento da informação em formato digital é exponencial e vai atingir os 35 Zettabytes[3] em 2020.

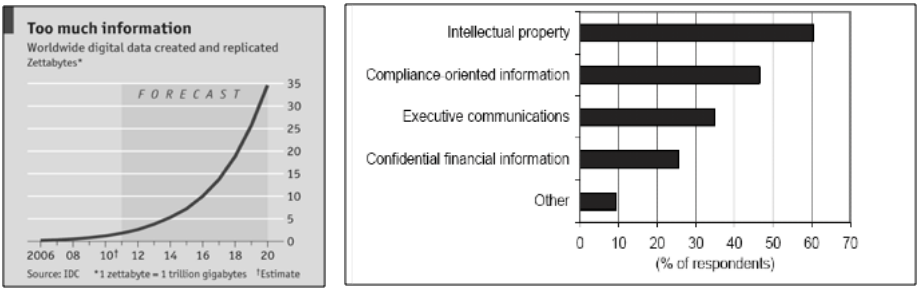
A crescente consciencialização dos riscos das fugas de informação foi despoletada por uma série de escândalos em que informações confidenciais foram divulgadas. Tal como a maioria desses casos demonstra, essas fugas são, muitas vezes, não o resultado de ações mal intencionadas, mas antes de ações de colaboradores que, sem o saberem, põem as suas organizações em risco. Isto pode acontecer quando colaboradores enviam para o exterior *e-mails* que contêm ficheiros ou documentos sem estarem cientes de que estes contêm informação confidencial. Outros exemplos são os

2 csSECURE, uma ferramenta da autoria da Critical Software.

3 1 Zettabyte = 1 Bilião de Gigabytes

colaboradores carregarem ficheiros com informação confidencial para as suas contas de *e-mail web-based*, ou copiarem ficheiros para dispositivos móveis e, assim, expô-los em ambientes que não são confiáveis. Tal como tem sido mostrado em estudos recentes, cerca de 60% das fugas de informação são relacionadas com Propriedade Intelectual, o que constitui para a maioria das organizações o seu bem mais valioso.

Figura 3 – Quantidade de informação e tipos de fugas de informação:
ICD Questionário de Proteção da Informação



Fonte: International Data Corporation (IDC, 2010). Disponível em http://www.idc.com.

A segurança da informação tem sido encarada como uma tarefa que envolve a proteção da informação sobretudo de ataques externos às infraestuturas e processos das organizações. Os *standards* de segurança e as melhores práticas (*e.g.* ISO/IEC 27002: 2005) são principalmente focados na proteção de um sistema de informação de eventos de origem externa, envolvendo a segurança de processos e da infraestrutura.

As situações que se referem a seguir dão conta da inconsciência (fugas de informação) de cooperadores ao lidarem com informação e tecnologias sensíveis para as organizações:

"Deutsche Bank Loses Hertz IPO Role Because of E-Mails
"Nov. 8 (Bloomberg) – Deutsche Bank AG, Germany's largest bank, lost its spot among the underwriters of Hertz Global Holdings Inc.'s initial public offering after an employee sent unauthorized e-mails to about 175 institutional accounts."
Carol Wolf and Christine Harper – November 8, 2006 14:51 EST
http://www.bloomberg.com

"MoD loses more laptops, USBs and 'secret files' (UK)
The Ministry of Defence has revealed that 658 laptops have been stolen over the past four years (…) The department also disclosed 121 of its USB memory sticks, some containing sensitive information, have been lost or stolen since 2004".
Siobhan Chapman | Published 17:06, 18 July 08
http://www.computerworlduk.com

> *"**Ponemon Institute Survey Finds 90 Percent of Businesses Fell Victim to Cyber Security Breach at Least Once in the Past 12 Months (…)***
> *A survey of US IT and IT Security professionals, conducted independently by Ponemon Institute and sponsored by Juniper Networks (NYSE: JNPR), found the threat from cyber attacks today is nearing statistical certainty and businesses of every type and size are vulnerable to attacks. (…) Overall, companies indicate that security breaches have cost them at least half a million dollars to address in terms of cash outlays, business disruption, revenue losses, internal labor, overhead and other expenses. Most respondents (59 percent) report that the most severe consequence of any breach was the theft of information assets, followed by business disruption (…) only 11 percent of respondents know the source of all network security breaches…"*
>
> NEW YORK, NY, Jun 22, 2011 (MARKETWIRE via COMTEX) – NExTWORK CONFERENCE – http://investor.juniper.net

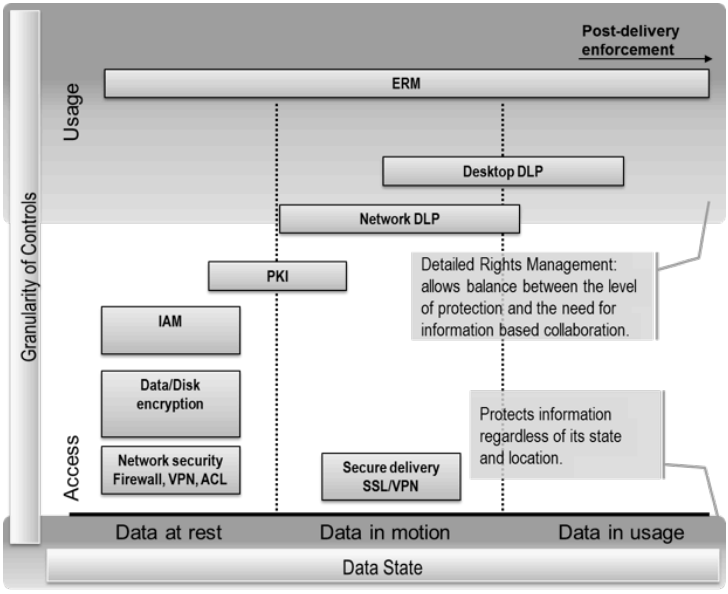
Afinal, proteger sistemas, infraestruturas e processos já não é, de todo, suficiente. As organizações devem proteger a informação em si mesma e assegurar que ela está bem protegida contra acesso não autorizado, independentemente do seu estado ou localização!

Solução de Alto Nível

A fim de evitar fugas de informação, esta deve estar protegida contra acessos não autorizados. A única forma de o assegurar é usar uma solução que aplique proteção persistente à informação e que viaja com ela, assegurando que os dados são protegidos independentemente do seu estado ou localização. Estas são soluções de segurança centradas nos dados.

Ao analizar a taxonomia das técnicas mais relevantes de segurança da informação (apresentadas na figura seguinte) é fácil perceber que a maioria das tecnologias foca-se na proteção dos dados num estado específico: em repouso – enquanto estão armazenados num computador ou disco rígido de rede; em movimento – quando estão a circular através da rede entre dois utilizadores ou máquinas; e em uso – quando estão a ser acedidos (a ser lidos, editados, imprimidos, etc.) pelos utilizadores.

Figura 5 – Taxonomia das tecnologias de segurança da informação



Fonte: International Data Corporation (IDC, 2010). Disponível em http://www.idc.com.

Pelo menos dois tipos de soluções de segurança têm uma maior visibilidade, tendo em conta a sua cobertura em termos de estados dos dados e funcionalidades: ERM e o DLP.

Enterprise Rights Management

Enterprise Rights Management – ERM – é uma tecnologia de segurança que aplica encriptação permanente aos dados, assegurando que a informação é protegida independentemente de estar em repouso, em movimento, ou em uso. Mesmo quando está a ser usada, a informação só é desencriptada na memória do computador e disponibilizada para a aplicação que a pretende usar. Enquanto a informação protegida por ERM está em uso, o ERM também aplica direitos detalhados sobre a sua utilização (bloquear certas ações como: imprimir, copiar para a área de transferência, exportar para outro formato, reencaminhar um *e-mail*, etc.).

Data Loss Prevention

As tecnologias de *Data Loss Prevention* – DLP – incluem uma ampla gama de soluções desenhadas para descobrir, monitorizar, proteger e controlar informação

sensível encontrada nos dados em repouso, dados em movimento, e dados em uso. Os sistemas são desenhados para detetar e prevenir o uso e a transmissão não autorizada de informação confidencial.

As soluções DLP baseadas na rede são normalmente instaladas no *gateway* corporativo. Estas soluções analizam o tráfego da rede como o *e-mail*, mensagens instantâneas, FTP, ferramentas *web-based* (HTTP ou HTTPS), e aplicações *peer-to-peer,* para detetar fugas de informação confidencial.

Soluções locais de DLP são normalmente instaladas em computadores de secretária, portáteis, dispositivos móveis, *pens* USB, servidores de armazenamento/ficheiros e outros tipos de repositórios de dados. Esta abordagem também inclui soluções que fornecem extração de dados e capacidades de classificação.

Soluções DLP de extração de dados são desenhadas para descobrir informações sensíveis em computadores de secretária, portáteis, servidores de ficheiros, bases de dados, gestores de documentos e registos, repositórios de *e-mail* e conteúdo e aplicações Web.

ERM *vs* DLP

Na tabela seguinte as vantagens e as desvantagens de cada tecnologia são apresentadas. Uma análise rápida revela que as desvantagens do DLP são exatamente as vantagens do ERM, e vice-versa.

Figura 6 – ERM vs DLP

	DLP	**ERM**
Sensibilização ao conteúdo	Descoberta de informação de conteúdo sensível e classificação	Não
Nível de imposição das políticas	Cumprimento ao nível do ficheiro, baseando-se em fatores tais como o tipo de dados; quando, onde e como podem ser acedidos; destinatários autorizados; tipo de informação	Persistente, proteção baseada na encriptação ao nível dos dados, independentemente de onde e por quem vão ser manuseados.
Nível de envolvimento do utilizador	Automático	Dependente do utilizador
Cobertura do ciclo de vida da informação	Aplicada apenas no acesso e utilização dos dados	Aplicada na criação dos dados e forçada através de todo o ciclo de vida da informação, incluindo proteção após transmissão da informação.

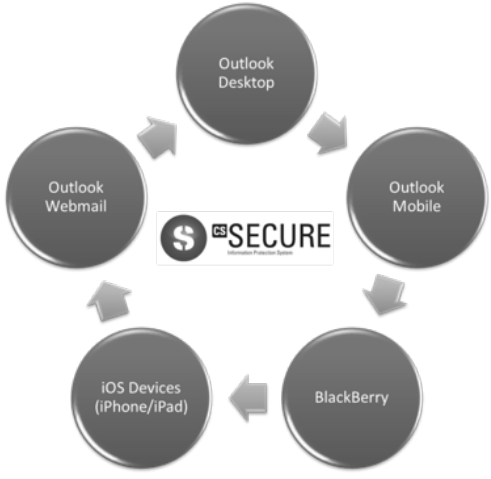
Há soluções que fornecem funcionalidades conjuntas de ERM e DLP, tirando partido dos pontos fortes de cada tecnologia de segurança. Entre empresas portuguesas que o fazem, são exemplo a *Critical Software* com o *software* csSSECURE.

Uma Solução de Segurança Centrada nos Dados

Entre outras soluções, seria interessante encontrar uma solução de proteção de informação integrada e transparente, que implemente o modelo de segurança multinível, permitindo que os utilizadores produzam informação usando as ferramentas de produtividade mais comuns (*office*, *e-mail*, dispositivos móveis, servidores de conteúdo, etc.).

Considera-se que a informação deve ser continuamente protegida. Ações como abrir, imprimir, editar, copiar, exportar, responder, reencaminhar devem ser ativadas ou desativadas de acordo com os direitos do utilizador sobre essa mesma informação. O *software* csSECURE conseguiu estes desideratos. Com ele a informação é protegida através de um algorítmo de encriptação permantente e os direitos que cada utilizador tem sobre a informação, são controlados durante o acesso.

Figura 7 – Plataformas de *e-mail* suportadas pelo csSECURE



Este *software* é baseado no modelo de segurança multinível que foi desenvolvido no mundo militar e assenta nas seguintes premissas:

- Toda a informação produzida numa organização é classificada de acordo com o seu nível de confidencialidade (e.g. interno, reservado, confidencial, secreto, …);

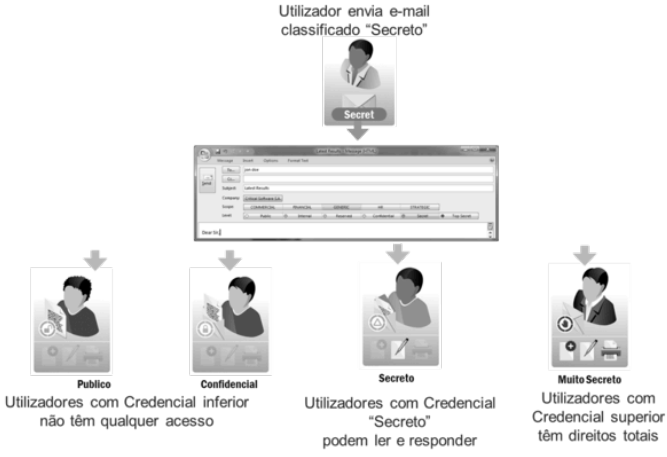
- Uma credencial de segurança é concedida a cada utilizador na organização;
- O acesso a informação classificada num determinado nível é apenas concedido a utilizadores com, pelo menos, uma credencial específica (*e.g.* informação classificada como confidencial apenas é acessível a utilizadores com a credencial confidencial ou superior).

O sistema csSECURE eleva este conceito base a um novo nível, adicionando duas novas derivadas:

- Quando é concedido acesso à informação a um utilizador, apenas certos direitos estão disponíveis para que este possa manipular os dados (e.g. o utilizador pode ser capaz de ler e editar a informação, mas tem as funcionalidades de imprimir ou copiar desativadas);
- Os níveis de classificação da informação podem ser agrupados em âmbitos de informação e estes em unidades organizacionais (e.g. a organização fictícia "Critical House" pode conter dois âmbitos [financeiro e gestão], e o âmbito financeiro pode conter três níveis de segurança: "secreto", "confidencial" e "reservado"). Este facto permite que utilizadores com diferentes perfis tenham acesso diferenciado à informação em função do seu âmbito (*e.g.* um utilizador poderá aceder a informação até ao nível "confidencial" num âmbito e apenas nível "reservado" nos restantes).

Neste tipo de abordgem o csSECURE permite a definição e a implementação de políticas de segurança da informação para gerir os direitos dos utilizadores de manipular e aceder à informação, de forma a mitigar o risco de ações não autorizadas sobre a informação, intencionais ou não. Um exemplo de políticas de segurança na solução csSECURE é apresentado na imagem seguinte.

Figura 8 – Exemplo de segurança multinível



Capacidades de Monitorização

As ações dos utilizadores sobre a informação protegida devem estar sujeitas a registo. Isto permite ao auditor de segurança saber, por exemplo, quais os ficheiros ou *e-mails* produzidos por cada utilizador e quando e como estes foram acedidos por outros.

No caso do *software* csSECURE por cada ficheiro ou *e-mail* protegido, o sistema gera um identificador único. Este identificador único pode ser usado para rastrear o ciclo de vida de um documento específico, obtendo todas as ações registadas sobre esse documento.

Este identificador único também pode ser usado para gerir uma lista negra de documentos, sendo que qualquer acesso posterior a estes documentos será negado. Isto é particularmente útil para gerir falhas de segurança identificadas dentro da organização e evitar acessos indevidos. Como a informação é permanentemente encriptada, o seu acesso depende de um processo de validação no servidor. Uma vez que o *software* está totalmente integrado com o sistema de ERM, é possível autorizar ou negar acesso a documentos individuais.

Porém, qualquer ferramenta de segurança de informação na sua própria configuração do sistema pode representar uma quebra de segurança porque o administrador pode conceder a utilizadores específicos direitos de acesso à informação da organização ou remover esses direitos. Para prevenir e monitorizar erros de administração, no csSECURE todas as tarefas de administração são registadas centralmente para auditorias futuras.

Identidade Avançada e Gestão de Acessos

É importante prevenir a perda de dados, aplicando à informação produzida dentro da organização técnicas de segurança. O csSECURE centra-se nos dados. Na maioria dos produtos de segurança, a identidade digital dos utilizadores no sistema é representada pelo *login* do utilizador. Se um utilizador ilegítimo assumir a identidade digital de um outro utilizador, este ganha acesso a todas as informações que deviam ser apenas disponíveis para o utilizador legítimo. A usurpação de identidade é um dos principais problemas em todas as soluções na área da segurança.

Os mecanismos de autenticação utilizados atualmente oferecem um nível razoável de proteção contra intrusos. No entanto, autenticação baseada em palavras-chave, ou até soluções de "autenticação forte" são fracas. Depois da fase de autenticação, não é necessária qualquer outra prova de identidade. Estes mecanismos possibilitam ataques oportunistas, especialmente de pessoas ligadas à organização

(*e.g.* deixar o computador ligado enquanto se está numa pausa para café ou em horário de almoço é uma oportunidade de ataque).

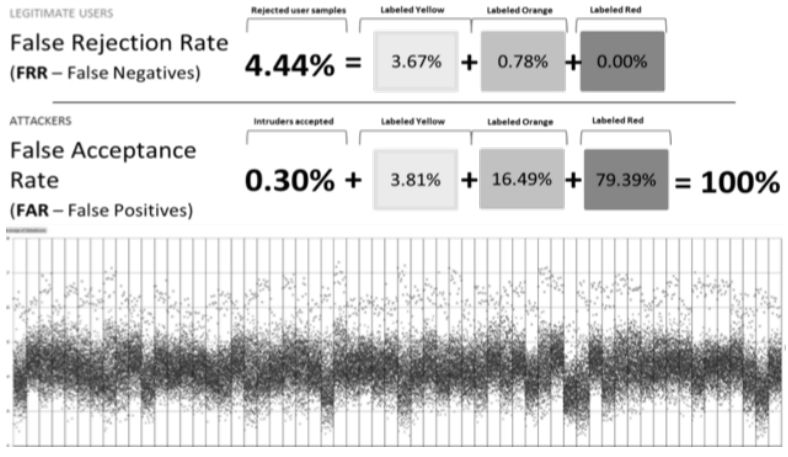
De maneira a prevenir a usurpação de identidade, necessitamos de uma técnica que contínua e passivamente monitorize as interações do utilizador, procurando indícios de intrusão. As soluções de Sistemas de Deteção de Intrusão Locais (*Host-based Intrusion Detection Systems*) satisfazem a maioria dessas condições; no entanto, as soluções atuais são focadas no sistema ao invés do utilizador. Ações que não ponham em causa a integridade do sistema são consideradas legais mesmo que executadas por utilizadores ilegítimos, pelo que continua a ser muito fácil executar ações prejudiciais e continuar indetetável.

Talvez uma das técnicas mais ajustadas será a identificação de características biométricas. O csSECURE dispõe de uma tecnologia, patenteada, que a realiza monitorizando as interações dos utilizadores com o computador, estendendo o conceito de IDS (Sistema de Deteção de Intrusões) para o nível de autenticação. O *Keystroke Dynamics* (que em português podemos apelidar de "dinâmica de digitação") é a técnica biométrica comportamental que satisfaz esta condição e que consiste na identificação e análise de padrões na atividade de digitação dos utilizadores, por forma a criar os seus perfis biométricos.

- Padrões de digitação estão continuamente a ser recolhidos após a fase de autenticação (providenciando autenticação contínua);
- É não intrusiva e transparente (a rotina do utilizador não é incomodada);
- É económica, dado que não necessita de nenhum equipamento especial.

Os resultados atuais da utilização desta tecnologia asseguram uma precisão de 99,7%.

Figura 9 – Eficácia do sistema de deteção de intrusos



Para melhor enquadrar o significado da Figura 9, seguem-se as definições de FRR e FAR.

- *False Rejection Rate*: probabilidade do sistema rejeitar indevidamente uma tentativa de acesso de um utilizador autorizado.
- *False Acceptance Rate*: probabilidade do sistema aceitar indevidamente uma tentativa de acesso de um utilizador não autorizado.

Pode-se então aferir que a solução rejeitou o acesso a 4,44% de utilizadores legítimos, sendo que a maioria desse valor (3,67%) apresenta variações muito ligeiras em relação ao seu modo de teclar mais comum. Por outro lado, apenas 0,3% utilizadores não autorizados foram aceites pela solução como sendo válidos.

Benefícios

A utilização de *software* desta natureza aumenta a consciencialização para a problemática da segurança da informação nas organizações, reforçando a necessidade de implementação de políticas de segurança, enquanto fornece às organizações meios para auditar e identificar falhas de segurança, reconhecendo tendências comportamentais e possíveis violações.

No caso do csSECURE são encontrados os seguintes benefícios:

Data Loss Prevention – aplicar políticas de segurança e regras na organização ajuda a prevenir, de maneira eficaz, a fuga de informação. As funcionalidades DLP permitem a aplicação de políticas de segurança, tais como a proteção automática de todos os ficheiros enviados via correio eletrónico ou transferidos para unidades externas.

Enterprise Rights Management - direitos detalhados sobre informação privilegiada, que bloqueia tentativas de fuga ou uso incorreto da informação interna para o exterior da organização. Ações como impressão, cópia, exportação para diferentes formatos ou reencaminhamento podem ser restringidas.

Gestão de políticas centralizada – Toda a gestão de políticas de segurança de informação é feita centralmente, através de uma consola *web.* É possível a transposição direta de políticas de segurança de informação e de procedimentos, assim como a importação de papéis e dados de perfil provenientes do diretório de utilizadores da organização.

Ampla gama de aplicações – O *software* suporta uma ampla gama de aplicações de produtividade e é facilmente extensível. A informação é encriptada de forma transparente e é acessível e eficazmente protegida na maioria das aplicações do *Office* utilizadas atualmente nas organizações. A informação está protegida, não interessando o local onde está armazenada, através de que canais foi transmitida ou onde está a ser acedida. Total proteção em repouso, em movimento e em utilização.

Sistema de deteção de intrusão do utilizador (inclui um sistema de deteção de intrusões que assegura uma taxa de confiabilidade de 99%. Esta técnica de biometria comportamental assegura uma autenticação contínua, é económica (não necessita de qualquer equipamento adicional) e é não-intrusiva, dado que não interfere nas tarefas normais do utilizador.

Capacidades de monitorização avançada – É possível monitorizar com detalhe o acesso à informação, o que possibilita que os auditores identifiquem desvios às políticas de segurança implementadas pelas organizações, detetando tendências comportamentais, configurando alarmes e medidas de prevenção. Permite que a organização obtenha uma panorâmica geral da utilização da informação.

Ciclo de vida da informação protegida – Com um identificador único de cada ficheiro e *e-mail* protegido é possível rastrear todos os acessos aos dados, analisando todo o ciclo de vida da informação protegida. Com base nesta funcionalidade, também é possível bloquear qualquer acesso a um ficheiro/*e-mail* específico, através da criação e gestão de uma lista negra.

Registos para auditoria dos administradores – A gestão do sistema permite dar acesso à informação a utilizadores não autorizados e modificar políticas de acesso e regras de DLP. Inclui um registo de todas as ações do administrador, prevenindo e monitorizando todos os possíveis erros de administração.

Considerações Finais

As soluções de segurança utilizadas atualmente são, tipicamente, centradas na rede ou na máquina, com objetivo de proteger a informação de ataques exteriores (*hackers*, vírus, cavalos de troia, etc.), mas falham no que diz respeito à segurança contra fugas de informação. De acordo com estudos recentes do IDC, as fugas de informação são maioritariamente acidentais (mais de 50%), e na maioria das vezes, para 26% das empresas, estes problemas podem significar custos diretos superiores a 100.000 US$.

As técnicas mais promissoras para controlar a fuga de informação são: ERM (*Enterprise Rights Management*) e DLP (*Data Loss Prevention*). ERM assegura que os dados são protegidos independentemente do seu estado (em repouso, em movimento ou em utilização), possibilitando também a criação de direitos detalhados para a informação (direito a imprimir, copiar, editar, exportar, responder, reencaminhar, etc.). O DLP assegura que as políticas da organização para lidar com informação digital são cumpridas por todos os utilizadores, definindo regras sobre a maneira como a informação deve ser manuseada e armazenada (*pen-drives*, *e-mail*, servidores da organização, etc.).

As desvantagens das soluções ERM (dependência do utilizador, carência de classificação automática e complexidade de administração) são precisamente as vantagens dos produtos baseados em DLP. O csSECURE, um produto com origem numa empresa portuguesa, é uma combinação das abordagens ERM e DLP, baseando-se no conceito de segurança multinível, que protege efetivamente as organizações contra fugas de informação permitindo, ao mesmo tempo, manter o controlo e monitorizar as ações executadas pelos utilizadores sobre a informação da organização, possibilitando rastrear a informação ao longo de todo o seu ciclo de vida.

Referências

International Data Corporation, IDC (2010). *Information Protection and Control*. Disponível em www.idc.com.

Kolodgy, Charles J. (2011). *Effective Data Leak Prevention Programs: Start by Protecting Data at the Source*. Framingham, MA: IDC Corporate USA.