CIBERSECURITY

Cybersecurity vs. Information Security (ISO27001/ISO27002)

OSMANY DANTAS RIBEIRO DE ARRUDA

2

LISTA DE FIGURAS

SUMÁRIO

2 CYBERSECURITY VS. INFORMATION SECURITY (ISO27001/ISO27002)

2.1 Considerações gerais sobre a Segurança da Informação

De acordo com o que foi discutido no primeiro capítulo, pode-se dizer que o conceito de *cybersecurity* é bastante amplo, porém ele remete claramente à preocupação com ferramentas, práticas, conceitos e políticas destinadas à **proteção da informação**, identificação e mitigação dos riscos aos quais essa informação possa vir a ser exposta – em última análise, para que seja garantida a continuidade do negócio.

Entretanto, o conceito de proteção, ou seja, de segurança dessa informação, pode não ser tão claro e intuitivo como inicialmente aparenta.

É procedimento comum em pequenas, e por vezes até em médias empresas, que a segurança da informação seja delegada a profissionais de TI (em sentido amplo), que não necessariamente são providos da visão e da especialização necessárias ao trabalho com a segurança da informação; isso leva a resultados invariavelmente aquém do esperado, a custos geralmente mais elevados do que o planejado e quase sempre com impacto indesejado sobre o negócio.

É notório também que, quanto mais seguro for o ambiente, menos operacional – ou, como popularmente descrito, “mais engessado” – este será; na medida em que a segurança da informação envolve, entre outros aspectos, a manutenção de **privilégios mínimos**, ou seja, a garantia de que um usuário comum não tenha privilégios suficientes, por exemplo, para instalar um *software*, uma vez que esta é claramente uma tarefa administrativa e, portanto, restrita ao administrador do sistema.

Diante disso, entretanto, alguns com conhecimento limitado em relação à segurança da informação poderão afirmar que tal prática produzirá impacto negativo sobre o negócio, na medida em que, ao limitar-se a execução até das tarefas mais triviais ao administrador do sistema, a produtividade do usuário final será consideravelmente prejudicada, levando o administrador a priorizar tarefas menores

em detrimento de afazeres mais relevantes, a fim de minimizar essa perda de produtividade, conduta também considerada como inadequada.

Em vista de tudo isso, os defensores de tal argumentação poderiam erroneamente concluir que, “no fundo, este problema pode ser facilmente resolvido” conferindo-se ao usuário privilégios mais elevados (talvez até irrestritos) no sistema.

Na verdade, entretanto, deve-se sempre ter em mente que não se trata simplesmente de conferir privilégios mais elevados ao usuário comum, mas sim conscientizá-lo e impedi-lo de executar ações administrativas, ou quaisquer outras que venham a extrapolar suas reais atribuições – no caso, a instalação de um *software*.

Nesse contexto, tomemos como exemplo uma situação hipotética, porém muito comum, na qual um usuário inicia a instalação de um *software* baixado da Internet e, em dado momento do processo de instalação, ele se depara com uma mensagem do sistema, semelhante à ilustrada pela figura “UAC solicitando permissão para instalação de software”.

Figura 2.1 – UAC solicitando permissão para instalação de software
Fonte: Malwarebytes.com (2020)

Um usuário comum certamente não terá condições de avaliar de maneira adequada o risco inerente à instalação de um *software* desconhecido em seu sistema, geralmente autorizando, em função disso, a continuidade da tarefa.

No caso específico do *software* indicado na figura “UAC solicitando permissão para instalação de software” (PDFBewerbungsmappe.exe), uma consulta a sites especializados revelará tratar-se do GoldenEye, *dropper* (inoculador) do Petya / Mischa (figura “PDFBewerbungsmappe.exe: dropper do GoldenEye”), abordado também no primeiro capítulo.

Portanto, pode-se afirmar que o uso seguro de um sistema ou de uma rede computacional exige também a clara definição dos **papéis e responsabilidades** de seus usuários, em todos os níveis de utilização, e não apenas nos mais altos.

Atividades administrativas em geral não devem, ao menos em princípio, ser permitidas a usuários comuns, pois exigem privilégios elevados, e a concessão de tais privilégios a quem não tem condições de avaliar de maneira adequada como utilizá-los de forma segura certamente produzirá resultados bastante diferentes dos esperados.

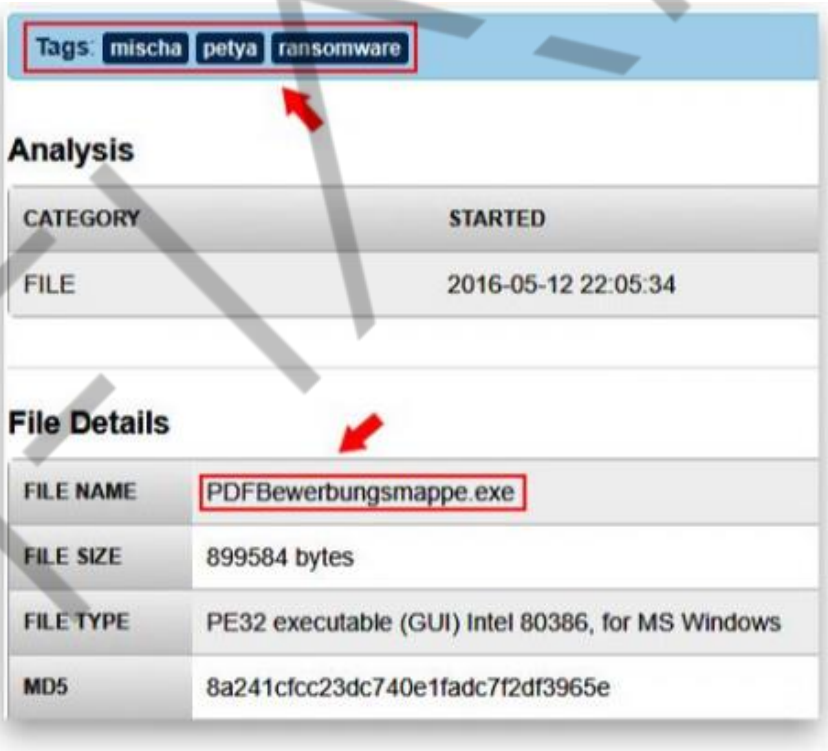

Figura 2.2 – PDFBewerbungsmappe.exe: *dropper* do GoldenEye
Fonte: Malwr.com (2020)

2.2 Definição de Segurança da Informação

É bastante comum a equivocada ideia de que a segurança da informação se resume a equipamentos e tecnologias, como, por exemplo, firewalls, IPS's e proxies, dentre outros.

Figura 2.3 – Citação de Bruce Schneier
Fonte: Google Imagens (2020)

Entretanto, de acordo com Bruce Schneier, renomado criptógrafo, especialista em segurança da informação e autor de várias obras nesse segmento, se você pensa que a tecnologia pode resolver seus problemas de segurança, é por que, na verdade, você não entende nem os problemas, nem a tecnologia.

A ISO/IEC 27002:2005 afirma que a informação é um **ativo altamente relevante para os negócios** de uma empresa e, assim sendo, deverá ser adequadamente protegida.

Não obstante, é notório ainda que a informação pode existir sob diversas formas, como, por exemplo, impressa ou escrita em papel, armazenada eletronicamente e falada.

Desse modo, a segurança da informação pode ser definida como a proteção da informação contra diferentes tipos de ameaça, com o objetivo de garantir a continuidade do negócio, minimizar os riscos aos quais este possa vir a ser exposto, aumentar o retorno sobre investimentos e as oportunidades de negócio (ISO/IEC 27002:2005).

À luz da ISO/IEC 27001:2005, observa-se que a referida proteção da informação pode ser inicialmente entendida como a preservação da **confidencialidade**, **integridade** e **disponibilidade** da informação, propriedades

eventualmente complementadas pela autenticidade, responsabilidade, não repúdio e confiabilidade.

Confidencialidade da informação significa que esta deverá ser revelada, ou estar acessível, unicamente aos que tiverem autorização para isso.

A Integridade é a propriedade que garante a exatidão e a plenitude da informação, o que não significa que esta não possa sofrer alterações ao longo de seu ciclo de vida, mas sim que tais alterações devem ser legítimas.

A Disponibilidade é a propriedade da informação de estar disponível e acessível quando necessário, aos que tiverem a devida autorização para isso.

Essa tríade retrata os pilares básicos da segurança da informação, sendo geralmente referenciada, simplesmente, como **CID** (figura “Pilares básicos da Segurança da Informação”).

É recorrente em ambientes com baixa maturidade corporativa, carentes de processos e controles adequados, e repletos de interpretações inadequadas da CID.

Considere-se, a título de exemplo, um servidor em que o serviço de compartilhamento de arquivos (ou qualquer outro) seja mantido em produção em período integral (24 x 7), independentemente de ser, ou não, requisitado por seus usuários.

A princípio, talvez alguns possam acreditar ser esse o conceito de disponibilidade, entretanto, observando-se o disposto pela ISO/IEC 27001:2005, conclui-se que, na verdade, a disponibilidade de qualquer serviço só é computada (e justificável) durante o período em que seus usuários legítimos o requisitarem em conformidade com as políticas de segurança da informação (PSI) da organização.

Assim sendo, a segurança da informação será maior se os serviços forem mantidos em produção de forma adequada, evitando que sejam desnecessariamente expostos (mesmo que somente na rede local), o que pode ser efetivado, por exemplo, por intermédio de *scripts* que automatizem a inicialização e a parada seletiva de cada serviço, em conformidade com as PSI.

Figura 2.4 – Pilares básicos da Segurança da Informação
Fonte: Google Imagens (2020)

A **autenticidade** tem como objetivo determinar a validade da transmissão, da mensagem e de seu remetente, a fim de permitir ao destinatário comprovar a origem e a autoria de um documento; enquanto o **não repúdio** tem como objetivo garantir que o autor não possa negar a criação e a assinatura do documento.

Tais propriedades vêm se tornando cada vez mais relevantes e evidentes, sendo implementadas por intermédio de técnicas de certificação e assinatura digitais, e de protocolação eletrônica de documentos.

De maneira simplificada, o certificado digital é a identidade digital da pessoa física ou jurídica no meio eletrônico, tendo como função garantir a **autenticidade**, **confidencialidade**, **integridade** e **não repúdio** das operações realizadas por seu intermédio, assegurando também a validade jurídica e permitindo que diversos serviços sejam realizados sem a necessidade da presença física – dessa forma, agilizando processos e reduzindo custos.

2.3 Introdução ao ROSI (*Return on Security Investment*)

O conceito de retorno sobre o investimento (ROI) aplica-se a todos os investimentos, não sendo exceção a segurança da informação.

De acordo com o programa de trabalho da ENISA em 2012, a fim de estimarem quanto deverá ser investido em segurança, os executivos precisam saber quanto a falta dela poderá custar ao negócio, e quais soluções mostram-se mais economicamente viáveis e satisfatórias.

Nesse contexto, tem-se o ROSI (retorno sobre o investimento em segurança da informação), cujo cálculo poderá responder questões financeiras essenciais, como: a organização está pagando excessivamente por segurança? Quanto a falta de segurança poderá impactar (financeiramente) sobre a produtividade? Quando os investimentos em segurança são suficientes? Essa prática ou esse dispositivo de segurança traz, efetivamente, benefícios?

Entretanto, há que se ressaltar que a abordagem financeira tradicional aplicável ao cálculo do ROI não é apropriada para avaliar iniciativas relacionadas à segurança da informação, uma vez que **investimentos realizados em segurança da informação geralmente não têm como resultado ou objetivo a obtenção de lucro, estando mais relacionados à prevenção de perdas**.

Em outras palavras, é esperado que os investimentos direcionados à segurança da informação minimizem os riscos aos quais os ativos da organização possam vir a ser expostos, e não a obtenção de benefícios – particularmente financeiros; ou seja, nesses termos a avaliação quantitativa do ROSI dá-se calculando quanto de perda para o negócio tais investimentos poderão evitar.

A figura “Curva de tolerância ao risco” representa a curva característica (genérica) de mitigação dos riscos relacionados à segurança da informação, em função dos investimentos recebidos.

Com base no perfil dessa curva é possível observar que investimentos reduzidos em segurança da informação agravam consideravelmente o risco, podendo também potencializar o impacto sobre o negócio produzido por eventuais incidentes de segurança.

É importante salientar ainda que esse impacto, normalmente, vai além das perdas financeiras diretas, ocasionando também desgaste da imagem corporativa e da reputação da empresa.

Em pesquisa publicada pela NortonLifeLock, dois terços dos consumidores em todo o mundo relatam estar mais alarmados do que nunca com sua privacidade

(67%) e estão muito preocupados com a possibilidade de sua identidade ser roubada (66%). Do total, 92% expressam pelo menos alguma preocupação no que diz respeito à privacidade de dados.

Já no outro extremo da curva, pode ser observado também que, a partir de determinado ponto, os riscos não poderão mais ser mitigados, independentemente dos investimentos realizados em segurança da informação, tornando clara a necessidade de determinação do ponto de equilíbrio entre risco e investimento (em segurança da informação), tendo-se como referência as necessidades e objetivos de negócio.

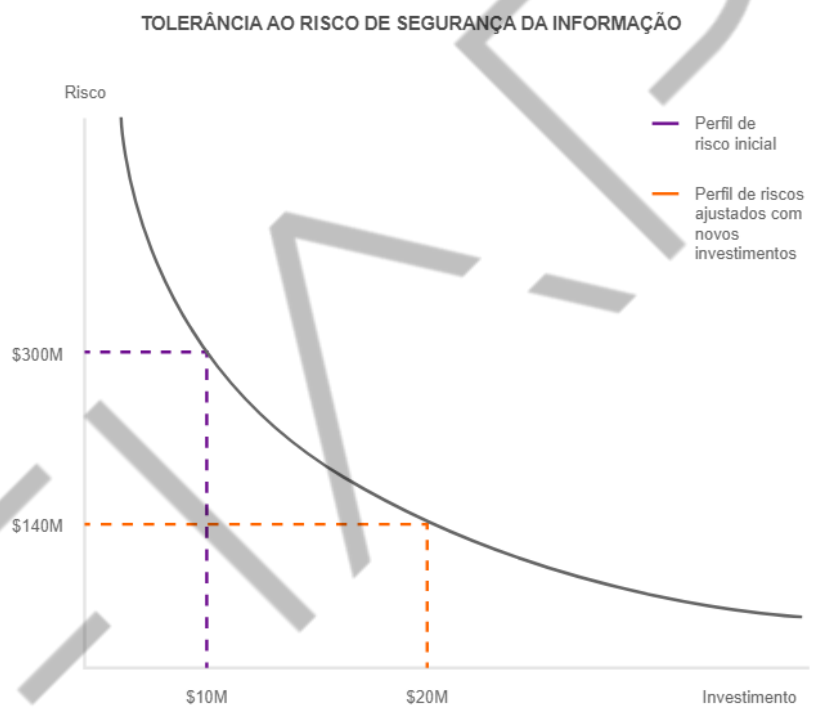

Figura 2.5 – Curva de tolerância ao risco
Fonte: Elaborado pelo autor (2020)

2.4 Princípios da segurança da informação

Diferentes técnicas e princípios deverão ser combinados a fim de que sejam compostas soluções adequadas e abrangentes, capazes de mitigar riscos e reforçar a segurança da informação.

O Sistema de Administração dos Recursos de Tecnologia da Informação – SISP, do Poder Executivo Federal, dentre outras reconhecidas instituições, coloca como estratégias fundamentais para proteção da segurança da informação:

2.4.1 Privilégios mínimos (*Least Privilege*)

Os usuários deverão ter seus privilégios para uso dos recursos informáticos limitados ao mínimo necessário para pleno desempenho de suas funções, evitando dessa maneira a desnecessária exposição a riscos, como, por exemplo, a instalação de códigos maliciosos, conforme anteriormente discutido.

O US-CERT acrescenta ainda que a concessão de privilégios excessivos a um usuário pode permitir que este venha a obter ou alterar informações de maneira indesejada, mesmo que involuntariamente. Logo, a cuidadosa delegação de privilégios poderá contribuir expressivamente para impedir que condutas impróprias ou inadequadas venham a comprometer algum dos pilares da segurança da informação e, ainda, para a redução dos riscos para o negócio.

2.4.2 Defesa em profundidade (*Defense in depth*)

A defesa em profundidade pode ser entendida como a implementação de um sistema defensivo **na forma de camadas**, no qual diferentes mecanismos de proteção se complementam, ampliando a abrangência e a efetividade desse sistema como um todo.

Tome-se como exemplo de defesa em profundidade a topologia ilustrada na figura “Defesa em profundidade”, onde um UTM é empregado para proteção da borda entre a rede confiável (LAN) e a rede não confiável (Internet).

Apesar de este ser capaz de inspecionar e disciplinar adequadamente o tráfego entre as duas redes, ele não é capaz de detectar ou proteger os hosts da rede local contra um ataque interno, como, por exemplo, um ataque de força bruta contra um servidor interno, desferido por um usuário mal-intencionado.

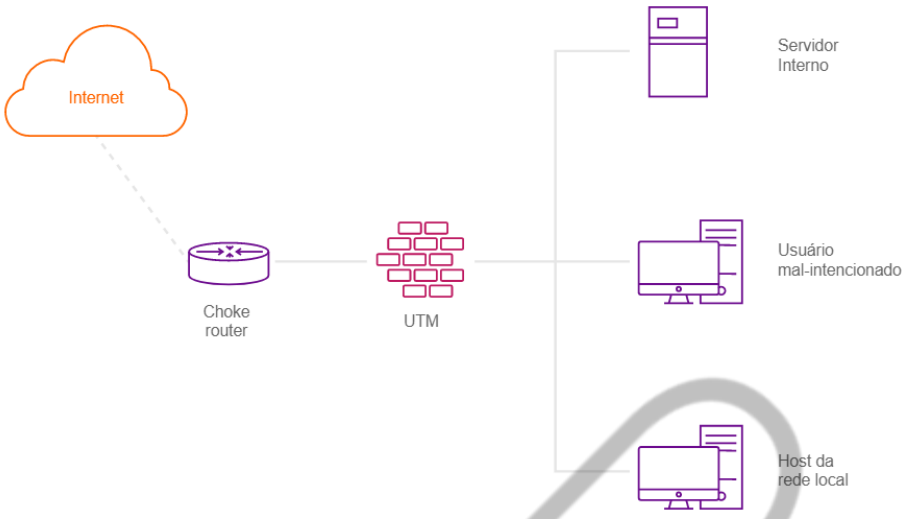

Figura 2.6 – Defesa em profundidade
Fonte: Elaborado pelo autor (2020)

Ainda na figura “Defesa em profundidade”, é possível observar que o UTM constitui a segunda linha de defesa do perímetro, sendo a primeira constituída pelo ***choque router***, o qual tem como função promover a filtragem inicial dos pacotes que entram e/ou saem da rede, sendo complementada por uma inspeção mais aprofundada por parte do UTM, o qual amplia ainda a superfície de proteção geral do sistema, implementando mecanismos de defesa adicionais, como sistemas de prevenção de intrusão (IPS) e filtragem de conteúdo, dentre outros.

A figura “Camadas da defesa em profundidade” representa o modelo conceitual da defesa em profundidade e suas camadas.

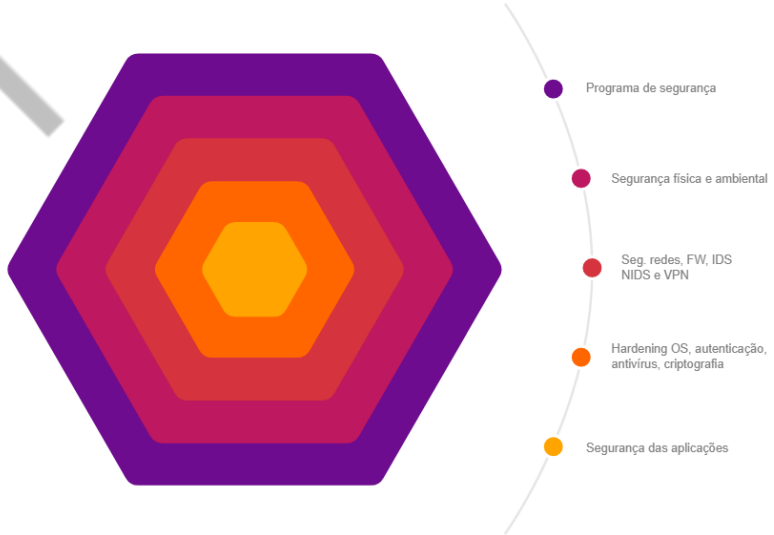

Figura 2.7 – Camadas da defesa em profundidade
Fonte: ISSA Brasil – CNASI (2020)

2.4.3 Elo mais fraco (*Weakest link*)

Os profissionais de segurança da informação geralmente a consideram como um encadeamento de estratégias e, assim sendo, tão forte quanto seu elo mais fraco, uma vez que atacantes certamente procurarão identificar e explorar os pontos mais vulneráveis dos sistemas de proteção, a fim de sobrepô-los.

Tomando novamente como referência a topologia representada na figura “Defesa em profundidade”, considere-se agora que o servidor interno deva ser acessado com segurança, também a partir da rede não confiável (Internet).

Dentre outras soluções possíveis, uma das mais simples e econômicas recai sobre a implementação de uma VPN (também uma funcionalidade do próprio UTM), com mecanismos de autenticação adequados, como, por exemplo, o uso de credencial forte, na qual nem o nome de usuário, nem a respectiva senha sejam de fácil dedução.

Aliando-se a uma credencial forte mecanismos de defesa complementares, como, por exemplo, o bloqueio da credencial utilizada após um determinado número de tentativas de acesso malsucedido, é mais provável que, para obtenção das credenciais do usuário um atacante venha a recorrer a técnicas de engenharia social, ao invés de ataques diretos ao serviço (por exemplo, dicionário ou força bruta).

2.4.4 Ponto de verificação (*Check point*)

Observando-se a topologia representada pela figura “Defesa em profundidade”, percebe-se que o conjunto <*choque-router* + UTM> constitui o único ponto para troca de tráfego entre a rede confiável (LAN) e a rede não confiável (Internet).

Desse modo, esse conjunto configura o chamado ponto de verificação (*check point*), por intermédio do qual **todo tráfego** que adentra, ou deixa, a rede confiável (LAN) poderá ser adequadamente inspecionado e submetido às políticas de segurança configuradas, minimizando a possibilidade de comprometimento de algum dos pilares da segurança da informação.

2.4.5 Segurança por obscuridade (*Security by obscurity*)

A segurança por obscuridade remete à dependência do segredo do projeto ou implementação, como forma de garantir sua segurança.

Simplificadamente, isso significa que, mesmo que um sistema, ou um de seus componentes, apresente vulnerabilidades, sua segurança ainda poderá ser (supostamente) mantida, enquanto tais vulnerabilidades não se tornarem conhecidas por terceiros.

O OWASP avalia que a defesa por obscuridade é um controle de segurança frágil, e que na maior parte das vezes falha quando é o único controle, não devido ao fato de que manter segredos seja uma má ideia, mas porque a segurança de um sistema importante não deve depender da ocultação de seus detalhes; por exemplo, a segurança de um aplicativo não deve recair sobre o segredo de seu código-fonte.

Haja vista o sistema operacional Linux, o qual, via de regra, é um software livre cujo código-fonte é aberto e amplamente disponibilizado, entretanto, quando adequadamente configurado, é um dos sistemas operacionais mais seguros e robustos disponíveis no mercado.

2.4.6 Princípio da simplicidade (KISS – *Keep It Simple, Stupid*)

O princípio da simplicidade é, por vezes, também referenciado como o “princípio do beijo” (KISS).

Ainda segundo o OWASP, a superfície de ataque e a simplicidade são intimamente relacionados, acrescentando ainda que certas práticas da engenharia de software privilegiam abordagens excessivamente complexas, em detrimento do que poderia ser um código relativamente mais simples e direto.

O problema decorre do fato de que a complexidade de um código dificulta seu pleno entendimento e, portanto, ao longo do processo de desenvolvimento, poderá vir a torná-lo vulnerável.

Considere, por exemplo, o *script* de um *firewall* (UTM) composto por centenas de linhas, e que um administrador ainda pouco familiarizado com esse *script* tenha

de adicionar regras específicas que permitam que uma nova aplicação entre em produção o mais rapidamente possível.

Considerando-se a complexidade do *script* (também em decorrência de sua extensão), associada ao tempo insuficiente para seu pleno entendimento, é provável que esse administrador comece a inserir e testar novas regras sem o devido critério, até obter o resultado desejado; comportamento que, embora inicialmente aparente ter resolvido adequadamente a demanda, pode na verdade estar criando vulnerabilidades que impactarão os mecanismos de defesa implementados por esse *firewall* (UTM).

Figura 2.8 – Conceito da simplicidade
Fonte: Google Imagens (2020)

2.4.7 Segregação de funções (*Separation of duties – SoD*)

A SoD é um controle clássico para resolução de conflitos de interesse e prevenção a fraudes, basicamente, mediante à restrição dos poderes de cada indivíduo e à criação de barreiras, fazendo com que mais de uma pessoa seja necessária para conclusão de uma tarefa.

O COBIT4.1 recomenda, no item PO4.11 Segregação de Funções:

"Implementar uma **separação de papéis e responsabilidades** que reduza a possibilidade de um único indivíduo subverter um processo crítico. A gerência também deve se certificar de que o pessoal esteja executando apenas tarefas autorizadas relevantes aos seus respectivos cargos e posições."

Não obstante, também a ISO/IEC 27001:2005 recomenda a segregação de funções (objetivo de controle A.10.1.3), a fim de garantir a operação correta e segura

de instalações para processamento da informação, e como forma de reduzir o risco de acessos não autorizados a um ativo, ou ainda, alguma modificação ou mau uso não intencional.

O OWASP cita como exemplo que um administrador deve ser capaz de inicializar e desligar um sistema, ou de implementar uma política de senhas; mas não deve ser capaz de fazer *logon* no sistema como um usuário superprivilegiado, e executar ações em nome de outros usuários.

Além dos princípios citados, o OWASP oferece ainda outras recomendações, como, por exemplo, a **Redução da Superfície de Ataques**, o que significa que cada funcionalidade adicionada a uma aplicação acrescenta também certo risco à aplicação como um todo; por exemplo, considere que uma certa aplicação *web* implemente um *help online* com função de busca, essa função poderá ser vulnerável a ataques de SQL *Injection*.

REFERÊNCIAS

ENISA – European Union Agency for Network and Information Security. **Introduction to return on security investment – helping CERTs assessing the cost of (lack of) security**. Disponível em: <https://www.enisa.europa.eu/publications/introduction-to-return-on-security-investment/at_download/fullReport>. Acesso em: 21 abr. 2020.

FERNANDES, J. H. C. **Gestão da segurança da informação e comunicações**. 2010. Disponível em: <https://dsic.planalto.gov.br/legislacao/3_Livro_GSIC_UNB.pdf/@@download/file/3_Livro_GSIC_UNB.pdf>. Acesso em: 21 abr. 2020.

_____. **Segurança de informação**. 2013. Disponível em: <http://www.egov.ufsc.br/portal/conteudo/segurança-de-informação>. Acesso em: 21 abr. 2020.

_____. **Segurança de informação**. Disponível em: <http://www2.tjal.jus.br/WebHelp/id_seguranca_da_informacao.htm>. Acesso em: 21 abr. 2020.

_____. **O que é certificado digital?** Disponível em: <https://www.certisign.com.br/certificado-digital/o-que-e-certificado-digital>. Acesso em: 21 abr. 2020.

_____. **Least Privilege**. 2013. Disponível em: <https://www.us-cert.gov/bsi/articles/knowledge/principles/least-privilege>. Acesso em: 21 abr. 2020.

_____. **Defense in Depth**. 2005. Disponível em <https://www.us-cert.gov/bsi/articles/knowledge/principles/defense-in-dept>. Acesso em: 21 abr. 2020.

_____. **Securing the weakest link**. 2013. Disponível em: <https://www.us-cert.gov/bsi/articles/knowledge/principles/securing-the-weakest-link>. Acesso em: 21 abr. 2020.

_____. **Security by design principles**. 2016. Disponível em: <https://www.owasp.org/index.php/Security_by_Design_Principles>. Acesso em: 21 abr. 2020.

_____. **Segurança da informação e comunicações**. Disponível em: <http://www.sisp.gov.br/faq_segurancainformacao/one-faq?faq_id=13941646#13971324>. Acesso em: 21 abr. 2020.

GREGG, J. et al. **Separation of duties in information technology**. 2017. Disponível em: <https://www.sans.edu/cyber-research/security-laboratory/article/it-separation-duties>. Acesso em: 21 abr. 2020.

MAGNUSSON, C.; MOLVIDSSON, J.; ZETTERQVIST, S. **Value creation and Return On Security Investments (ROSI)**. Disponível em: <https://ai2-s2-

pdfs.s3.amazonaws.com/3f84/55ec9ee0e16a4fb50a903262bdd1c3d639d3.pdf>. Acesso em: 21 abr. 2020.

MCGUINESS, T. **Defense in depth**. 2001. Disponível em: <https://www.sans.org/reading-room/whitepapers/basics/defense-in-depth-525>. Acesso em: 22 abr. 2020.

NORTON. **NortonLifeLock Cyber Safety Insights Report**. [s.d.]. Disponível em: <https://us.norton.com/nortonlifelock-cyber-safety-report>. Acesso em 21 abr. 2020.

TCU. **Boas práticas em segurança da informação**. 4. ed. 2012. Disponível em: <http://www4.planalto.gov.br/cgd/assuntos/publicacoes/2511466.pdf>. Acesso em: 3 out. 2017.

GLOSSÁRIO

UTM	Acrônimo para Unified Threat Management (Gerenciamento Unificado de Ameaças), é uma solução abrangente, criada para o setor de segurança de redes, sendo teoricamente uma evolução do *firewall* tradicional, reunindo em um único dispositivo várias funções de segurança, tais como: filtragem de pacotes, sistemas de prevenção de intrusões, antivírus, VPN, filtragem de conteúdo.
LAN	Acrônimo para Local Area Network, normalmente traduzido apenas como “rede local”, é uma rede que interliga computadores restritos a uma área limitada, como, por exemplo, uma localidade da empresa ou uma escola, dentre outras.
Firewall	É um dispositivo de segurança para proteção de um computador, ou rede de computadores, que tem por objetivo aplicar uma política de segurança. Em sua origem, é um dispositivo com foco na filtragem de pacotes e nos estados da sessão.
Choke router	É um roteador que executa também a filtragem inicial dos pacotes que o atravessam, em geral operando conjuntamente com um UTM e constituindo a primeira linha de defesa da LAN.
VPN	Acrônimo para Virtual Private Network (Rede Privada Virtual), consiste de uma rede de comunicações privada estabelecida sobre uma infraestrutura de comunicações pública, com objetivo de prover ao usuário acesso remoto seguro ao serviço desejado, ou interligar com segurança diferentes localidades de uma empresa.
SQL Injection	Consiste na exploração de vulnerabilidades de sistemas que utilizam a linguagem SQL para interação com suas bases de dados.