Análise CIDAL – Detalhamento

Uma das causas de investimentos equivocados em Segurança da Informação é a inexistência de uma prévia análise CIDAL. CIDAL é um acrônimo para os atributos principais da informação (CID – a tríade da Segurança da Informação – Confidencialidade, Integridade e Disponibilidade), somados aos atributos considerados complementares: Autenticidade e Legalidade. Seus significados, de forma bastante resumida, são:

- Confidencialidade – é uma propriedade da informação que define a dimensão do grupo de pessoas e sistemas que necessitam possuir acesso à informação. Quanto menor este grupo, mais protegida ele deve ser. Naturalmente, "dimensão" aqui é um termo relativo à própria empresa, então se apenas em torno de 5 pessoas precisam ter acesso à uma determinada informação em uma empresa com 5000 funcionários, ela é altamente confidencial. Esta análise é melhor realizada com o auxílio de uma escala definindo graus de confidencialidade e a dimensão aproximada do número de componentes máximo para cada grau. Exemplo:
  - ✓ Ultra-secreta – 5 pessoas em 5000;
  - ✓ Secreta – 50 pessoas em 5000;
  - ✓ Confidencial – 500 pessoas em 5000;
  - ✓ Reservada – 5000 pessoas em 5000 (neste caso, apenas as pessoas da empresa precisam conhecer a informação); e
  - ✓ Pública ou ostensiva – além de não haver restrições, em alguns casos é interesse da empresa que o público conheça a informação.

  O próximo passo é a definição de Políticas de Segurança para cada tipo de grau. Muitas vezes informações ultra-secretas são tão estratégicas para a empresa que devem ser particionadas entre os membros do grupo, de forma que para comprometer o seu sigilo, todos do grupo precisam estar corrompidos.

- Integridade – Esta é uma propriedade controversa. Por definição, a garantia de integridade busca evitar que TERCEIROS, ou seja, elementos não autorizados a acessar a informação, consigam alterá-la ou corrompê-la. Mecanismos de garantia de integridade não são eficazes quando a alteração é feita pelo elemento que possui as credenciais para fazê-lo;
- Disponibilidade – Este atributo está ligado a uma demanda temporal que a empresa possui para tomada de decisões, para as quais as informações são essenciais. Se não existem, precisam ser construídas para que uma decisão adequada possa ser tomada, e isso pode ser inviável para o negócio. Além disso, caso as informações existam, e rápidas decisões precisam ser tomadas, existe a demanda de alta disponibilidade, definindo a necessidade de mecanismos de redundância de equipamentos e enlaces, replicação de bases de dados, etc. É obvio que este atributo só entra em discussão após assegurada a confidencialidade e,principalmente a integridade da informação. De nada adianta ter disponível uma informação corrompida;
- Autenticidade – É considerado atributo complementar por ser necessário a todos os outros. Se a informação é confidencial, serão necessários mecanismos auxiliares de autenticidade para garantir que a pessoa ou sistema que está acessando a informação realmente é quem diz ser e está autorizado a acessá-la. Enquanto para garantia de confidencialidade usa-se,por exemplo, a criptografia, para autenticidade, mecanismos de senhas, biometria e outros podem ser adotados. Da mesma forma, uma informação só deve estar disponível para quem tenha direitos de acessá-la, envolvendo assim a necessidade de procedimentos de autenticidade; e
- Legalidade – Atualmente, a sua ausência é a causadora da maioria dos grandes incidentes de segurança das empresas. Pessoas habilitadas para acesso à informação se corrompem e usam os seus direitos físicos e tecnológicos de acesso à informação para obterem vantagens financeiras. A ausência de mecanismos coercitivos legais, tanto em nível federal/estadual/municipal quanto corporativo, criam um ambiente propício às fraudes. A incapacidade das empresas em lidar com funcionários que se corrompem e cometem atos contrários aos interesses das empresas. Na prática, ao invés de demissão por justa causa com acionamento da polícia, as empresas fazem acordos com estes funcionários, dispensando-os e ainda os indenizando pela dispensa, ironicamente cumprindo a lei para dispensas de funcionários sem justa causa. É

fundamental que situações ainda não previstas em lei sejam adequadamente tratadas em códigos de postura ética corporativos, que os mesmos sejam divulgados, acordados de forma contratual com os colaboradores e que efetivamente seja cumprido e cobrado. Punições devem ser clara e explicitamente definidas e, principalmente, aplicadas quando ocorrerem incidentes. Para evitar problemas com a justiça do trabalho, sugere-se que um mecanismo interno de investigação do caso, com amplo direito de defesa seja utilizado. Provas e evidências testemunhais e documentais devem ser agregadas a este processo.

A identificação da natureza do atributo comprometido em cada tipo de incidente é fundamental. A partir daí é possível definir os mecanismos de segurança que podem ser usados para redução do risco de comprometimento do negócio. A técnica básica é identificar qual tipo de mecanismo de segurança efetivamente poderia ter evitado o incidente.

Observe o caso a seguir:

Caso Renault – Jornal "O Globo" – RJ – Janeiro de 2011

Renault suspende três executivos por espionagem

Especula-se que segredos seriam sobre carro elétrico

Do El País*

• PARIS. Na última segunda-feira, os seguranças do complexo tecnológico Renault Technocentre, na cidade francesa de Guyancourt, pediram que três altos executivos da montadora deixassem o local. Acusados de espionagem, ou seja, de vender informações importantes — supostamente sobre o projeto do carro elétrico da Renault —, os três estão suspensos sem remuneração até o fim das investigações, a cargo do Departamento Jurídico da empresa. O ministro da Indústria, Eric Besson, confirmou o ocorrido ontem em entrevista à rádio RTL e falou em guerra comercial:

— Isso mostra os riscos que nossas empresas enfrentam em termos de espionagem industrial e inteligência econômica.

O Estado francês tem 15% de participação na Renault. A montadora não revelou a identidade dos executivos. Mas, segundo o jornal "Le Parisien", um deles seria Michel Balthazard, de 56 anos, há 30 na Renault, membro do Conselho de Administração e encarregado, entre outras coisas, dos futuros modelos de automóveis. Outro seria seu braço direito, Bertrand Rochette, e o terceiro, Matthieu Tenenbaum, vice-diretor do programa do carro elétrico da empresa. Todos trabalham no Technocentre.

As suspeitas surgiram em agosto, após denúncias de que informações sigilosas estariam sendo vendidas a concorrentes, e uma investigação interna foi iniciada. O diretor jurídico da Renault, Christian Husson, afirmou em nota que os acontecimentos são muito graves.

Sem confirmar que as informações seriam sobre o carro elétrico, ele disse haver "provas de que três executivos violaram a ética da Renault, conscienciosa e deliberadamente colocando em risco os ativos da empresa". Husson acrescentou que todas as opções legais estão sendo examinadas e que a empresa não fará mais comentários. ■

(*) *Com agências internacionais*

Em uma primeira abordagem, é comum identificar o incidente de segurança como de Confidencialidade, uma vez que informações estratégicas de um projeto de inovação teriam sido vendidas. Outros talvez indicassem o atributo Autenticidade, alegando que os altos executivos não deveriam ter acesso às informações técnicas, mas apenas aos aspectos necessários ao negócio, à atividade executiva. Ambas as abordagens estão incorretas. É óbvio que os aspectos Confidencialidade e Autenticidade deveriam ter sido revistos e robustecidos de forma compatível com o impacto de um incidente como o que ocorreu, mas como a pergunta foi: no cenário apresentado, qual foi o atributo da informação comprometido, a resposta correta é: LEGALIDADE. Um dos executivos envolvidos seria o responsável pelos futuros modelos, naturalmente lhe garantindo acesso autenticado às informações do mesmo, e da mesma forma, as eventuais proteções de confidencialidade não protegeriam a informação, pelo fato dos envolvidos fazerem

parte do grupo considerado pertencente aos funcionários que necessitam ter acesso à informação. Apenas ações punitivas claras e eficazes poderiam desestimular este tipo de incidente. Vamos ver outro exemplo:

PEDRO DORIA

Um dia, o hacker bate à porta

A manhã faz duas semanas que usuários do PlayStation Network, a rede que interliga jogadores do console de videogames da Sony, está fora do ar. Não é um sistema pequeno: são 77 milhões de usuários. A promessa é de que tudo lentamente volte a funcionar nos próximos dias. Mas a queda, motivada por um ataque hacker, levanta muitas perguntas sobre privacidade e as conveniências de uma vida passada online.

A segurança da rede do PlayStation foi quebrada entre 17 e 19 de abril. Dados que incluem identidade, senhas e endereços dos 77 milhões de usuários foram levados pelos invasores. Embora eles tenham tido acesso também ao banco de dados com números de cartões de crédito, a empresa acredita que estejam seguros. Estavam encriptados. (Por que o resto não foi igualmente encriptado? É uma excelente pergunta que a Sony não conseguiu responder).

Foi a própria Sony que decidiu derrubar o sistema, no dia 20. Sem explicações claras. Descobriu que a falha explorada pelos hackers continuava lá e, aparentemente, deu trabalho resolver. Não envolvia só a rede de gamers. Também o Qriocity, sistema que vende música e filmes sob demanda nos EUA, Europa e Ásia, foi atingido. Ou seja: afeta uns tantos americanos com televisões modernas que já alugam filmes via internet.

Há apenas uma semana, a discussão na tecnologia envolvia Apple, Google e os celulares que acompanham os passos de seus usuários. É desconfortável que empresas colham dados particulares da clientela sem deixar claro que isso ocorre.

Mas empresas deste porte têm ações na bolsa, estão sujeitas a processos, quando antipáticas demais perdem fregueses. O risco maior destes grandes bancos de dados é que a segurança não é perfeita. Outros, não sujeitos à moderação das leis do mercado ou do Estado de direito, às vezes conseguem botar as mãos em nossos dados. Foi o que ocorreu no caso da Sony.

O PlayStation Network é um dentre muitos exemplos da computação em nuvem. Este é o caminho que a internet está tomando. Se nos últimos anos o hábito foi de manter toda nossa informação em computadores pessoais, mudou. E não à toa. Nossa vida digital não se limita mais a computadores pessoais. Tem o computador de casa e o do trabalho. O celular inteligente. O tablet. Cada aparelho faz parte do cotidiano em momentos diferentes. E precisamos que todos estes aparelhos tenham acesso ao mesmo conjunto de dados. A solução é colocar tudo na internet.

Os dados de 77 milhões de usuários da Sony foram violados. É caso grande, mas não isolado

Quem migrou para e-mail online, como Gmail ou Hotmail, está na nuvem. Quem usa Google Docs, idem. Parte da decadência da Microsoft, que vendia software, se explica pelo rumo da computação para a nuvem. As redes sociais todas só fazem sentido na nuvem. Rádios online, que começam a se popularizar? Nuvem.

Daí o risco duplo. Se temos informação demais em computadores alhures, precisamos confiar que a segurança é plena. Só que mesmo uma empresa do quilate da Sony, hoje, não é capaz de garantir tal segurança. Quando o pior acontece, sequer com transparência podemos contar. A Sony explica muito pouco. O segundo risco é na vida prática. Quando um serviço da nuvem sai do ar, perdemos tudo por completo. No caso, uma turma ficou sem jogar videogames. Mas poderia ser o e-mail, ou uma planilha. O impacto é grande.

No início de abril, uma penca de servidores da Amazon.com ficou fora do ar, afetando vários serviços que incluem a rede social Foursquare. A Amazon também silenciou. Em janeiro, clientes americanos da telefônica AT&T que tinham iPads 3G também viram suas identidades violadas. O caso do PlayStation é maior, mas não isolado.

Na expressão da revista britânica "The Economist", são as dores de crescimento da computação em nuvem. Maior estabilidade há de vir no futuro. Se a Justiça e os consumidores punirem como cabe, transparência também virá. Até lá, no entanto, a vida estará sujeita a turbulências, e a conclusão de sempre permanece inevitável. A engrenagem da internet não permite privacidade. A alternativa é sair da rede.

E-mail para esta coluna: *pedro.doria@oglobo.com.br* siga a coluna: @pedro.doria

O texto é claro em identificar a razão do incidente de segurança: dados sigilosos NÃO estavam criptografados. Isso significa que houve quebra da confidencialidade, já que o mecanismo não existia. Se ele existisse, mas fosse quebrado através de alguma técnica específica para isso, também seria incidente de confidencialidade. É comum a identificação deste incidente como de autenticidade, uma vez que os hackers ganharam acesso ao sistema, o que apenas poderia ser feito após uma autenticação. Não é o caso. Apenas seria incidente de autenticidade se o invasor tivesse quebrado uma proteção desta natureza, e ela foi simplesmente ignorada (ineficaz, portanto) por existirem vulnerabilidades nos sistemas que permitem isso.

É importante pensar na Segurança da Informação em camadas. Cada informação sensível deve ter proteções específicas para cada atributo que represente risco. Na prática, é comum que as corporações invistam apenas em algumas "camadas", deixando outras a descoberto, e é aí que as ameaças atuam: onde a Segurança é falha.

Se persistirem dúvidas, selecionem artigos sobre incidentes, tentem aplicar a técnica aqui descrita e mandem para mim. Terei prazer em analisar e emitir a minha opinião.

Abraços,

Fred Sauer, D.Sc.
fsauer@gmail.com