PRISM: de olho em tudo o que você faz na internet

Um ex-agente da NSA, a Agência de Segurança Nacional dos Estados Unidos, revelou que o país monitora tudo o que eu, você ou praticamente qualquer outra pessoa faz na internet. Chamado de PRISM, o projeto contaria com a colaboração de empresas de telefonia e também de algumas das maiores companhias digitais do mundo, como Facebook, Microsoft, Apple e Google.
Os segredos foram trazidos à tona por Edward Snowden, um engenheiro e administrador de redes que trabalhava no órgão governamental. Snowden denunciou as práticas de espionagem em uma entrevista porque, segundo ele, “quem deve decidir se os governos devem ou não investigar o que as pessoas comuns fazem na internet são os próprios cidadãos.”
De forma geral, o PRISM seria um programa de vigilância constante e em tempo real realizado pela NSA, a Agência de Segurança Nacional dos Estados Unidos, e que estaria monitorando ligações telefônicas, atividades realizadas com cartões de crédito e tudo o que fazemos na internet, seja o envio de e-mails, conversas por meio do Facebook ou a simples navegação aleatória por sites de notícias, por exemplo.
A denúncia de Snowden diz que a NSA teria acesso direto e irrestrito às informações de nove dos principais sites e portais dos Estados Unidos. Slides entregues pelo ex-agente mostrariam diversas empresas como Yahoo!, Google, Microsoft, Facebook, PalTalk, YouTube, Skype, AOL e Apple como “colaboradores”.

Normas de Segurança de Dados Corporativos
A segurança da informação está diretamente relacionada com proteção de um conjunto de informações, no sentido de preservar o valor que possuem para um indivíduo ou uma organização. São características básicas da segurança da informação os atributos de confidencialidade, integridade, disponibilidade e autenticidade, não estando esta segurança restrita somente a sistemas computacionais, informações eletrônicas ou sistemas de armazenamento. O conceito se aplica a todos os aspectos de proteção de informações e dados. O conceito de Segurança Informática ou Segurança de Computadores está intimamente relacionado com o de Segurança da Informação, incluindo não apenas a segurança dos dados/informação, mas também a dos sistemas em si.
Atualmente o conceito de Segurança da Informação está padronizado pela norma ISO/IEC 17799:2005, influenciada pelo padrão inglês (British Standard) BS 7799. A série de normas ISO/IEC 27000 foram reservadas para tratar de padrões de Segurança da Informação, incluindo a complementação ao trabalho original do padrão inglês. A ISO/IEC 27002:2005 continua sendo considerada formalmente como 17799:2005 para fins históricos.

A Segurança da Informação se refere à proteção existente sobre as informações de uma determinada empresa ou pessoa, isto é, aplica-se tanto as informações corporativas quanto às pessoais. Entende-se por informação todo e qualquer conteúdo ou dado que tenha valor para alguma organização ou pessoa. Ela pode estar guardada para uso restrito ou exposta ao público para consulta ou aquisição
.
ATRIBUTOS BÁSICOS, SEGUNDO OS PADRÕES INTERNACIONAIS (ISO/IEC 17799:2005)

Confidencialidade - propriedade que limita o acesso a informação tão somente às entidades legítimas, ou seja, àquelas autorizadas pelo proprietário da informação.
Integridade - propriedade que garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação, incluindo controle de mudanças e garantia do seu ciclo de vida (nascimento,manutenção e destruição).
Disponibilidade - propriedade que garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pelo proprietário da informação.
Autenticidade - propriedade que garante que a informação é proveniente da fonte anunciada e que não foi alvo de mutações ao longo de um processo.
Irretratabilidade - propriedade que garante a impossibilidade de negar a autoria em relação a uma transação anteriormente feita
Conformidade - propriedade que garante que o sistema deve seguir as leis e regulamentos associados a este tipo de processo.

Sendo estabelecidas as normas de segurança para os dados, as empresas, passaram a procurar possíveis “falhas” e “brechas”, que poderiam acarretar em comprometimento das informações, armazenadas em seus Data Centers, e servidores locais. Dessa forma foram levantadas as principais causas de vulnerabilidade das informações em um BD, e medidas que devem ser adotadas para melhorar a segurança do BD.

10 Principais causas de vulnerabilidades em Sistemas de Banco de Dados

- Privilégios excessivos ou esquecidos.
- Abuso de privilégio
- SQL Injection
- Malware
- Auditoria fraca
- Exposição de mídia de storage
- Exploração de vulnerabilidades e configurações fracas de banco de dados
- Dados sensíveis sem politicas de segurança.
- DoS - Negação de Serviço
- Pouca experiência dos profissionais na área de segurança.

Algumas medidas que devem ser adotadas para melhorar a segurança do Banco de Dados

- **Separação de Tarefas**
  O conceito de separação de tarefas (SOD, Separation of Duties) determina que as tarefas de administração devem ser divididas entre vários usuários, em vez de ficarem a cargo de uma única pessoa com plenos poderes. Dividir tarefas como administração, segurança e operações diminui o risco de os usuários abusarem de seus privilégios e também reduz a área da superfície de ataque no caso de contas invadidas.

- **Usuários Nomeados**

  Os administradores jamais devem compartilhar contas por praticidade (aliás, por nenhum outro motivo). Contas compartilhadas impedem a responsabilização, aumentam o risco e basicamente tornam impossível auditar as atividades do usuário. Cada usuário de uma organização deve ter uma conta individual nomeada, explicitamente associada ao seu nome. Cada conta nomeada é então vinculada a privilégios personalizados, selecionados de acordo com a função dessa pessoa dentro da organização. Regras de gravação de logs de auditoria baseadas em políticas podem ser definidas e a atividade do usuário pode ser auditada individualmente.

- **Gestão de Contas SysDBA**

  A conta SYS do proprietário do banco de dados (SYSDBA) é um privilégio administrativo que fornece acesso irrestrito ao banco de dados, como uma conta ROOT no gerenciamento do sistema operacional. É simplesmente poder demais para que qualquer usuário o tenha de forma permanente. De fato, muitos dos próprios administradores de banco de dados pensam que ter os privilégios da conta SYSDBA os coloca em uma indesejável posição de potencial responsabilidade caso algo saia errado. Sendo assim, o uso dessa conta e de seus privilégios precisa ser administrado e monitorado de perto, e tais privilégios só devem ser concedidos quando for absolutamente necessário, tal como durante atualizações e correções do banco de dados. Tire proveito de um sistema de gerenciamento de contas privilegiadas combinado a um sistema de gerenciamento de mudanças e designe uma janela de tempo de uso específica a fim de gerenciar de perto o privilégio SYSDBA. Recomenda-se o uso de controles de segurança compensatórios

quando contas SYS/SYSDBA são usadas. Um exemplo de tal controle seria exigir fluxos de trabalho de aprovação secundários (a regra das duas pessoas).

- **Privilégio Mínimo**

  A Separação de Tarefas (SOD) separa pessoas, processos e contas, mas você não consegue aplicá-la quando todos os usuários e contas têm todos os privilégios. Depois de ter a SOD implementada, aplicar o princípio do privilégio mínimo limita cada usuário e cada conta a ter apenas os privilégios necessários para as operações do dia a dia. Em suma, esse modelo recomenda que os usuários recebam apenas o conjunto mínimo de privilégios necessários para que realizem suas tarefas relacionadas ao trabalho, e nada mais. Lembre-se de remover privilégios quando não forem mais necessários.

- **Proteção da Auditoria**

  Os logs de auditoria são necessários para emissão de relatórios de conformidade e para perícia em caso de violações ou outros eventos adversos. Faça um registro irrefutável das ações realizadas por contas nomeadas, incluindo “CREATE USER”, “CREATE ANY TABLE”, “ALTER SYSTEM” e “ALTER SESSION”, e adicione informações contextuais, como endereço IP e hora do evento. Os registros de auditoria ajudam as organizações a identificar usuários perigosos, otimizar as auditorias e simplificar a conformidade.

Entendendo Melhor Banco de dados em Nuvem (Cloud DB)

Existem diversas vantagens que uma solução em nuvem tem em relação ao armazenamento tradicional, quando nas mãos de um provedor de serviços de nuvem experiente.

Manter seus dados em seu servidor local, em seu escritório, é comparável a encher dinheiro em um colchão. Em última análise, sua melhor alternativa é colocá-lo no banco. Quando você procurar por uma empresa de armazenamento de dados, encontre uma que nunca foi *hackeada* ou comprometida, que passe por auditorias regulares do governo e mostre um longo histórico de sucesso.

A internet continuará ativa, independentemente da catástrofe, isso porque não é fisicamente vulnerável à destruição. Se alguma coisa acontecer com seu escritório, incêndio, inundação, roubo ou corrupção de servidor antigo, você poderá voltar a trabalhar rapidamente, pois seus dados estarão disponíveis na internet. Em muitos escritórios, uma porta trancada é a principal defesa para proteger o equipamento de TI, arquivos importantes e dados pessoais e comerciais. Em contraste, os centros de dados dos provedores de serviços de nuvem têm defesas de segurança física em várias camadas. Essas instalações são policiadas por guardas, câmeras, senhas de entrada sofisticadas e portas abóbadas. Tais instalações são complexas para garantir a integridade física dos dados armazenados.

Quando os dados são armazenados na nuvem, funcionários, vendedores e visitantes estão fisicamente separados dos dados de missão crítica da empresa. Assim, os dados permanecem seguros, pois é muito difícil, para não dizer impossível, que algum de seus colaboradores, por exemplo, que esteja por alguma razão desapontado com a organização, corrompa seus arquivos, baixe vírus ou destrua seu hardware de armazenamento, ou mesmo que terceiros tropecem em dados e os usem negativamente. O risco humano diminui. Todos os laptops, desktops e outros equipamentos eletrônicos irão um dia parar de funcionar. E quando acontecer, você ainda terá trabalho a fazer. Você pode voltar ao negócio imediatamente com um backup de dados em nuvem, recuperação de desastres e acesso a área de trabalho remota. Desta forma, a

computação em nuvem protege mais do que os seus dados: ele protege a continuidade de seus negócios.

Algumas Vantagens Específicas do Banco de Dados em Nuvem

- **Redução de Custos**

  Quando não se tem um banco de dados na nuvem, é comum que as empresas tenham que optar por softwares e hardwares mais complexos. E a manutenção desses servidores físicos é altamente onerosa. Já com o cloud computing, os custos são reduzidos. Afinal, o prestador de serviços é quem fornece espaço, profissionais e infraestrutura. Ou seja, é possível escalar somente os recursos necessários para determinado período e também diminuir gastos com pessoal especializado.

- **Garantia de Segurança no Armazenamento**

  Muitos gestores ainda têm receio quanto ao uso do banco de dados na nuvem no que diz respeito à segurança dos dados armazenados. No entanto, essa ferramenta pode tornar o armazenamento mais confiável, por contar com recursos como firewalls e criptografia. Também existem as senhas, que regulam o acesso aos dados, protegendo-os de estranhos. Além disso, por não depender de hardwares, a empresa fica menos vulnerável aos riscos de roubos e acidentes. Assim, o resgate de arquivos é muito mais fácil.

- **Facilidade em Eventuais Adaptações**

  É possível modificar a infraestrutura de tecnologia rapidamente, a qualquer momento. Isto é, caso a demanda por armazenamento de dados seja alterada, o negócio pode solicitar mudanças na disponibilidade de recursos e ser prontamente atendido. O ajuste às necessidades de uso é útil principalmente para produtos/serviços de caráter sazonal.

Conclusão

Com essa pesquisa pude ver, que, a informação é o bem mais precioso que uma empresa pode ter, e o vazamento de dados confidenciais, podem ser prejudiciais a ponto de gerar até guerra entre nações. Aprendi também que, os dados armazenados em servidores locais, são mais vulneráveis do que se pode imaginar quando não se analisa os riscos de forma adequada e que privilégios para acesso ao BD devem ser sempre mínimos, ou seja, apenas o necessário para que o trabalho seja executado de forma satisfatória. A computação em nuvem trouxe muitas novidades e tendências ao mercado atual, com isso surgiu também o Banco de Dados em nuvem, que para mim, parece ser uma grande tendência para as empresas por trazer muitas vantagens em diversos aspectos, como segurança, e economia.