

# O lado analógico da segurança digital

A segurança da informação de uma empresa vai muito além de simples firewalls e antivírus. Sua maior fraqueza geralmente se encontra nas pessoas. É necessário pensar a esse respeito.

por Eduardo Moura

Iwan Beijes - www.sxc.hu

Todos os administradores de rede se preocupam com segurança. Mantêm os servidores devidamente atualizados, as regras de detecção de intrusão em dia, assim como as assinaturas de antivírus, e estão sempre atentos às vulnerabilidades das estações de trabalho (quer sejam Linux, Mac ou Windows®). Porém, existe um imenso risco de segurança que não é devidamente tratado nas companhias: as pessoas.

Muitos invasores aprenderam que algumas (às vezes muitas) pessoas sentem-se felizes em ajudar o próximo. Aproveitando-se dessa felicidade, elaboram planos minuciosos de ataque social a empresa.

Com uma informação inocente fornecida por um funcionário, uma outra por um segundo funcionário e mais algumas por seus colegas, o atacante obtém um “esboço” de mapa da empresa. Com esse mapa, ele pode solicitar, com aparência de total legitimidade, um acesso à rede, uma caixa postal e até mesmo cartões de visita com seu nome.

Além disso, invasores com o perfil de engenheiros sociais são mais preparados do que a média, e pensam em recompensas diferentes daquelas

dos “script kiddies” convencionais. Esses invasores são motivados por fatores econômicos e têm um foco mais apurado, ou seja, sua meta não é dominar milhões de sistemas, mas apenas um sistema que contém as informações desejadas.

O quadro acima parece assustador, mas é plausível em organizações que encaram a segurança da informação como produto em vez de processo. Softwares e hardwares de última geração não protegem as empresas contra a falta de treinamento e aculturação de suas equipes.

Este artigo, o primeiro de uma série de dois, discute algumas providências “analógicas” para aumentar o nível de segurança de suas informações digitais, baseadas em oito perguntas-chaves.

## 1. Identificação

*Como as pessoas identificam as outras dentro de sua empresa?*

Em empresas cada dia maiores e mais dispersas, é comum que os funcionários não se conheçam. É prudente, nesse caso, desenvolver processos de “validação de identidade”. Por exemplo, ao receber a ligação de um “novo funcionário”

solicitando informações, peça seu número dizendo que vai retornar os dados para ele em alguns momentos. Em seguida, confirme com a área de segurança ou de recursos humanos se a pessoa efetivamente é quem diz ser.

Esse tipo de procedimento garante que as duas pessoas, até que se estabeleça um conhecimento mais próximo, compartilhem informações tranqüilamente.

## 2. Dados sensíveis

*Qual o tratamento dado às informações sensíveis dentro da empresa?*

Sua empresa possui algum processo formal de destruição de informações sensíveis? Se os colaboradores não tiverem uma exata noção do que é sensível e de como manejar este material, ele pode acabar nas mãos de atacantes e servir de base para a construção de um ataque social ainda mais indetectável. Fragmentar relatórios com material sensível é uma prática desejável. Além disso, é preciso educar as pessoas no tratamento de todas as peças de informação disponíveis.

Um email contendo dados confidenciais passado via Internet é transmitido no formato “texto plano” e,

portanto, passível de interceptação eletrônica. Por esse motivo, esse procedimento deve ser evitado ao máximo. Essa consciência se adquire através da sensibilização.

### 3. Vazamento

*Existe uma checagem do que é gravado em mídias removíveis pelos usuários?*

Dispositivos de armazenagem estão cada vez maiores e mais acessíveis aos consumidores. É importante que toda a gravação de arquivos em dispositivos como estes, conectados a computadores da empresa, seja monitorada ou restrita. Num mundo onde a informação tem valor cada vez maior, deixar que pessoas mal intencionadas saiam com ativos preciosos da empresa é um risco que deve ser considerado e, quando necessário, combatido.

### 4. Treinamentos

*Como são ministrados e repetidos os treinamentos sobre segurança da informação para os colaboradores?*

Treinar e esclarecer as pessoas a respeito dos riscos de segurança é muito mais importante do que investir muito em tecnologia de segurança. O elo mais fraco na cadeia de segurança da informação são os ativos humanos. Não à toa, é sobre eles que grande parte dos ataques mais elaborados ocorre, justamente através da engenharia social. Ter uma estratégia clara de treinamento e reforço das políticas de segurança da informação representa garantir uma redução sensível nos incidentes de segurança da empresa.

### 5. Procedimentos

*Os procedimentos técnicos que precisam de interação dos usuários são claros e conhecidos?*

Esse é um ponto de “cruzamento” do ataque, até aqui social, com o mundo digital. Depois de um esforço detalhado, o atacante pode se “mimetizar” como um colaborador da área de tecnologia e entregar um programa malicioso quase indetectável dentro de seu ambiente computacional. Este tipo de ameaça tem um efeito devastador, pois sua detecção em geral é tardia e muito mais difícil, já que não há evidência de comportamento anormal.

### 6. Tabu

*Os colaboradores são orientados quanto aos assuntos que não devem ser discutidos ou referenciados em espaços públicos (tanto o mundo físico quanto a Internet)?*

Quando um grupo de pessoas da mesma empresa se encontra em um ambiente público, existe uma tendência natural de conversarem sobre assuntos da empresa. Um atacante determinado pode aproveitar uma oportunidade dessas para obter alguns termos, jargões ou outras informações relevantes que servirão para elaborar um ataque social. O treinamento de segurança deve alertar as pessoas para evitar discutir assuntos sensíveis da empresa em locais públicos sem os devidos cuidados.

### 7. Descarte

*Qual a destinação de componentes eletrônicos (discos rígidos, computadores completos, unidades de fita e fitas magnéticas) que não são mais úteis à empresa?*

Com a digitalização cada vez maior dos ativos de informação das empresas, a destinação final de resíduos de tecnologia deve ter uma atenção toda especial. Atacantes podem revirar resíduos como estes em busca de pedaços de informação, e com eles montar uma “história plausível”. Com essa história, pode-se abrir uma porta na

sua organização e, através dela, tomar conhecimento de preciosos segredos sem ninguém perceber.

### 8. Até já

*Como as pessoas deixam suas mesas ao sair do trabalho?*

Uma situação corriqueira que vemos nos escritórios modernos é o abandono de pequenas notas com números de telefones, recados, números de contas bancárias, senhas (sim, até senhas) em mesas e monitores nas empresas. Um atacante com a motivação correta pode explorar o serviço de limpeza e obter algumas cópias dessas notas, usando-as para elaborar sua história de fachada.

Talvez essa preocupação pareça exagerada. Afinal, há apenas um agente 007. Mas a versão mais simples desse argumento é bem mais convincente: contratos importantes que devem ser assinados no dia seguinte podem simplesmente desaparecer, prejudicando a empresa e fazendo-a perder um cliente importante. Orientar as pessoas para que mantenham as mesas limpas depois do expediente ou mesmo durante uma ausência mais prolongada (horário de almoço, por exemplo) evita a exposição de informações sensíveis a olhos indevidos.

Essas perguntas têm como objetivo levantar as principais questões com respeito à segurança da informação dentro das empresas. A continuação deste artigo será publicada na próxima edição da **Linux Magazine**, e discutirá mais detalhadamente por que essas questões de segurança devem ser levadas a sério mesmo em empresas pequenas que atuam em mercados teoricamente seguros. ■

#### Sobre o autor

**Eduardo Moura** (eduardo.moura@telway.com.br) é consultor em segurança da informação e governança de TI. É entusiasta do Software Livre e atua na Telway Tecnologia.