SEGURANÇA DA INFORMAÇÃO

ASPECTOS NÃO TECNOLÓGICOS

Este artigo chama a atenção para fatores humanos relativos à segurança da informação que são muitas vezes subestimados, particularmente em projetos ou atividades com grande emprego de tecnologia, mas que no final fazem grande diferença no sucesso de uma empreitada.

Flavio Moura Santos*

ATAQUES DE "WORMS"

No início da internet comercial no Brasil, houve um período em que era comum as empresas sofrerem interrupção de serviços por conta de ataques de vírus tipo "worm".(1) Estes vírus, introduzidos inadvertidamente por algum usuário desprotegido ou descuidado, espalhavam-se automaticamente pelas máquinas vulneráveis, levando-as à paralisação e ao engarrafamento da rede de comunicação por excesso de tráfego. Quanto mais integrado o ambiente da empresa, maior era o estrago. Frente a essa situação de vulnerabilidade, as equipes responsáveis pela informática trabalhavam, em geral, de forma reativa. Não raro gastavam muitas horas à noite e final de semana adentro eliminando os vírus das máquinas em um esforço repetitivo e insano para trazerem de volta à normalidade o ambiente computacional da empresa atacada.

A situação típica das empresas neste início da internet comercial era a incipiência, ou mesmo a ausência, de governança, padrões e normas de segurança de informações adequados ao ambiente distribuído e aberto onde grassavam os ataques. O conhecimento, procedimentos e normas herdados dos ambientes centralizados não eram suficientes para neutralizar os efeitos dos ataques de vírus. O desespero nessa situação demandava soluções rápidas e eficazes. O que fazer?

ESTUDO DE CASO

O caso a seguir é a resumida história de como uma grande empresa nacional venceu esta batalha contra ataques de vírus tipo "worm".

A empresa possuía uma rede totalmente integrada, conectando dezenas de milhares de computadores em todo o território nacional, estando a metade, aproximadamente, localizada no Rio de Janeiro, e o restante espalhado pelos demais estados da Federação. Um percentual considerável destes equipamentos atendia unidades industriais trabalhando em regime 24x7, entre as quais muitas de pequeno porte, que contavam com computadores mas não com técnicos de informática em seus quadros. O atendimento a essas unidades era feito, sempre que possível, remotamente. Entretanto, em algumas situações, tornava-se necessário o envio de um técnico para efetuar o atendimento presencialmente, como por exemplo em alguns ataques de vírus.

A rede, totalmente integrada, permitia o acesso direto a qualquer computador, em qualquer unidade da empresa, o que facilitava sobremaneira o espalhamento de vírus tipo "worm". Alguns ataques conseguiam contaminar uma quantidade tão grande de máquinas que paralisavam o tráfego de dados em algumas localidades, exigindo o envio de técnicos para

eliminação do vírus e restauração do ambiente. Cortar completamente a comunicação de uma unidade para evitar que, a partir dela, o vírus se espalhasse era muito delicado, pois interromperia também o tráfego útil de dados, causando prejuízos operacionais à organização.

A empresa estava convivendo há alguns meses com ataques tão frequentes que as equipes técnicas já haviam normalizado sua convivência com essa situação. Era-lhes natural e esperado passar noites e finais de semana trabalhando para restaurar o ambiente. A única proposta de solução era investir na contratação de uma camada adicional de segurança de "end point".

A alta administração da empresa, preocupada e sem ver perspectivas concretas de solução, começava a participar diretamente na coordenação do tratamento dos incidentes. Neste contexto, foi criada uma gerência com função específica de coordenar as ações relativas à segurança das informações. Foi nomeado um gestor com perfil técnico, mas que não estava envolvido diretamente no tratamento dos incidentes.

O levantamento inicial promovido pela nova gerência identificou a seguinte situação:

- a solução de antivírus cobria aproximadamente 50% das máquinas;
- a administração do antivírus não era centralizada;[2]
- não havia normas que determinassem a instalação e uso do antivírus, ou soluções de segurança em todas as estações;
- não havia procedimentos formalizados de resposta a incidente;
- não havia equipe formalizada de resposta a incidente; e
- a coordenação e integração com o fabricante da solução de antivírus eram deficientes.

O problema visível

Constatou-se que a solução de antivírus não estava sendo eficaz o suficiente para proteger todo o ambiente da empresa, e nem poderia sê-lo, dada sua baixa cobertura. Era também comum a reinfecção pelo mesmo vírus.

Atingir uma cobertura grande o suficiente para que ela se tornasse eficaz implicaria criar normas, procedimentos e também instalar a solução antivírus em milhares de equipamentos Brasil afora. Essa operação toda demandaria um tempo longo demais frente aos impactos operacionais aos quais a empresa estaria sujeita até a sua conclusão.

Primeiro grande aprendizado

O primeiro aprendizado com o cenário exposto foi a constatação que "o foco na tecnologia pode desviar a atenção da natureza do problema". Isso porque, não seria eficaz, neste caso, investir em uma nova solução tecnológica, fosse substituindo a atual, fosse adicionando uma nova camada de segurança, se não houvesse um crescimento significativo da abrangência da nova solução.

Portanto, o problema em questão não era tecnológico. Era humano, de gestão, cultural, de conscientização, normas, procedimentos, delegação.

Segundo grande aprendizado

É impossível prever tudo o que pode acontecer de errado, ou de onde virá, ou como será um possível ataque: um sistema deve ser projetado a partir da condição de falha. Esta lição é fator crítico de sucesso para não depender da sorte e diminuir danos advindos de eventos não previsíveis. Isto é particularmente importante no caso de sistemas cuja falha, ou comprometimento, possa provocar danos humanos.

Não adianta investir exageradamente em proteção, cobrir-se de todos os recursos tecnológicos possíveis e com isso acreditar que o sistema não vai parar.[3] A abordagem correta é garantir a continuidade operacional da empresa, mesmo em situações de falhas, e não apenas esperar que novos investimentos venham a resolver o problema.

Solução

Considerando o cenário apresentado, buscou-se uma solução em duas frentes: a primeira, de caráter emergencial, visava minimizar os prejuízos causados pelos ataques; a segunda, de médio prazo, tratava a causa-raiz do problema, tendo em vista a baixa eficácia da solução de proteção.

Na primeira frente, a prioridade de ação foi formalizar uma equipe nacional de resposta a incidentes; criar e aprovar procedimentos de monitoração, comunicação e acionamento deste time. Além disso, aumentou-se a integração com o fornecedor da solução de antivírus, que prestava suporte localmente, garantindo seu acionamento imediato, quando necessário.

Na segunda frente, o foco voltou-se para garantir o melhor uso da tecnologia da informação, com o estabelecimento de um processo de governança de segurança das informações, campanhas de conscientização e a formalização de normas que determinavam o uso das soluções de segurança em todo o ambiente e sua administração centralizada.

CONCLUSÕES

Agir apenas reativamente a incidentes, sem entendimento dos problemas que permitem a sua ocorrência, é como tirar água de um barco furado sem consertar o furo. Neste caso, ou os recursos para tratamento e eliminação do problema são extraordinariamente superdimensionados, ou afunda-se junto com o barco.

Em geral, porém, não é possível esperar a solução do problema – é necessário tratar de forma emergencial o incidente, o que seria equivalente a tirar água do barco para que se possa consertar o furo. Para tanto, é necessário ter equipes treinadas, disponíveis e rapidamente acionáveis, além de algum esquema de monitoramento para que o incidente seja prontamente identificado e mitigado, a fim de ganhar o tempo necessário para resolver o problema.

Deve-se considerar também que as pessoas se adaptam rápida e imperceptivelmente a novas situações e que um olhar externo pode enxergar problemas e saídas não visíveis àqueles que estão imersos em um determinado cenário.

E, por fim, constata-se que o tratamento de crises demanda foco. No caso estudado, a criação de uma gerência com fim específico e a nomeação de um gestor externo trouxeram mais foco e uma nova visão à situação, facilitando a identificação e solução de problemas que estavam sendo vivenciados pelos técnicos. ■

NOTAS

(1) "worm" é uma espécie de vírus que tem a característica de se espalhar automaticamente pela rede procurando computadores vulneráveis. Ex.: "Love letter", "Code Red", "Nimda".

(2) A importância da administração centralizada da solução de antivírus, bem como qualquer outra solução de segurança, era particularmente relevante no caso em função do ambiente de rede ser totalmente integrado sem barreiras de proteção entre as redes dos diversos órgãos.

(3) Quem quiser se aprofundar sobre este tema, recomendo o livro "A lógica do Cisne Negro", de Nassim Nicholas Taleb e Marcelo Schild, que apresenta as características do comportamento humano por trás deste tipo de atitude.

* Engenheiro, integrante do Grupo de Interesse em Ciência, Tecnologia, Engenharia, Matemática e Inovação (CTEMI) do Clube Naval