SEGURANÇA DE DADOS:
O QUE É PRECISO PARA PROTEGER INFORMAÇÕES EMPRESARIAIS?

FORTES
tecnologia em sistemas

Introdução

No começo de maio de 2017, inúmeras empresas dos cinco continentes, especialmente da Europa, sofreram um ciberataque criminoso em massa que sequestrou computadores corporativos e impediu que funcionários tivessem acesso a seus dados. Isso evidenciou **a necessidade cada vez maior de se investir em segurança da informação** dentro das empresas, sob o risco de sofrer prejuízos financeiros elevados.

Aliás, segundo a pesquisa International Business Report da Grant Thornton – The Global Impact of Cyber Crime, em 2016 os prejuízos com ataques virtuais chegaram a **US$ 280 bilhões** no mundo. O estudo foi feito pela quinta maior organização do ramo de auditoria, consultoria e outsourcing do Brasil, junto a 2500 líderes de empresas de 36 economias.

Ter a marca afetada, perder dados sigilosos de clientes e ficar à mercê de criminosos virtuais também são problemas que podem afetar empresas que não se preocupam ou não investem o suficiente na proteção de seus sistemas. Por isso, é fundamental buscar soluções e práticas que garantam a proteção e a integridade das informações corporativas.

Neste e-book, você verá quais os principais riscos e as ações necessárias para se proteger dos ataques virtuais que podem comprometer todo o ambiente organizacional. Portanto, se você deseja se informar mais sobre como se precaver, não deixe de conferi-lo!

Quais são as ameaças e modalidades de problemas?

Existem muitas ameaças e modalidades de ataques que podem comprometer os sistemas de uma empresa.

A seguir, selecionamos alguns dos principais tipos que mais prejudicam as corporações, podendo comprometer o sigilo dos dados e a segurança das informações organizacionais. Confira:

1. INVASÃO DE SISTEMAS

Os cibercriminosos utilizam diversas estratégias para invadir sistemas empresariais, para que possam copiar ou roubar dados sigilosos.

Dessa forma, podem conseguir obter informações ou executar ações que possibilitem desviar valores em ambientes virtuais, como ocorreu com o banco central de Bangladesh em fevereiro de 2016.

Na ocasião, US$ 81 milhões foram roubados e o prejuízo poderia ter passado de 1 bilhão se não tivesse ocorrido um erro numa palavra usada num código pelos hackers.

Além disso, o ciberataque trouxe prejuízos à segurança do **sistema SWIFT**, que é responsável pela gestão de operações financeiras e bancárias a nível mundial.

Problema semelhante ocorreu com a Sony em 2014, quando hackers invadiram os sistemas da empresa e disponibilizaram, em sites de download, filmes de seu catálogo que ainda nem haviam sido lançados.

Os cibercriminosos também divulgaram informações sigilosas, como salários e números da previdência social de milhares de funcionários da empresa, causando problemas ao RH corporativo e à organização como um todo.

2. SEQUESTRO DE DADOS

Como comentado na introdução, o mundo presenciou um grande ataque virtual no começo de maio de 2017. Na ocasião, foi usado a técnica de ransomware, em que "ransom" significa "resgate" e "ware" deriva do sufixo de "Malware".

Em geral, nessa modalidade, um vírus criptografa todos os dados de um computador, que passa a exibir na tela um pedido de resgate, um valor a pagar para que seus dados sejam descriptografados e possam ser utilizados novamente.

O vírus usado nesse ataque, chamado de **Wannacry** chegou também ao Brasil, tendo afetado a Petrobras, o Instituto Nacional de Seguridade Social (INSS) e alguns tribunais.

3. DERRUBADA DE SISTEMAS

Outra modalidade de ataque que tem causado muitos transtornos é a de **negação de serviços** (DDdoS), pois se tornaram muito populares no país. Segundo um estudo feito no último trimestre de 2015 pela Nexusguard, companhia de segurança digital, o país ficou na sexta posição mundial de ataques do tipo. Ao todo, foram 3690 ações identificadas.

Nessa modalidade, as incursões são realizadas por múltiplos computadores que, em uma ação coordenada, atacam simultaneamente um único sistema. O objetivo é sobrecarregá-lo e torná-lo indisponível para seus usuários, podendo afetar portais, serviços online, sites etc. Eles são muito empregados para a remoção de websites e páginas virtuais do ar.

Talvez, o maior problema desse tipo de ataque seja o fato de ele **vir acompanhado de outras ações mais perigosas**, servindo mais como distração para uma invasão.

4. RISCOS DE CONFIDENCIALIDADE E PROBLEMAS DE SEGURANÇA DE DADOS DURANTE UMA TROCA DE INFORMAÇÕES

Na troca de dados e informações, como acontece com e-mails e mensagens instantâneas, é fundamental utilizar uma **tecnologia de criptografia**. Dessa forma, é possível aumentar a confidencialidade e evitar que sejam interceptadas por indivíduos mal-intencionados.

5. PERDA DE INFORMAÇÕES DEVIDO A PANES OU FENÔMENOS NATURAIS

A perda de informações devido a panes em equipamentos ou a fenômenos naturais, como enchentes, também pode trazer problemas às empresas.

Isso é capaz de deixar sistemas inoperantes por dias, além de provocar retrabalho na recuperação dos arquivos perdidos, como veremos adiante.

Que prejuízos podem causar?

Veja melhor alguns exemplos de prejuízos que as ações criminosas virtuais podem acarretar para uma empresa:

1. PREJUÍZOS FINANCEIROS

Ataques virtuais a organizações podem ocasionar **muitos prejuízos financeiros**.

Por exemplo, o já citado caso da Sony causou uma perda de cerca de US$ 200 milhões para os cofres da empresa.

Nesse sentido, engana-se quem acha que somente grandes corporações são afetadas, pois as médias e pequenas também estão suscetíveis aos cibercriminosos, que podem extorquir tais empresas para não vazarem os dados capturados e, desse modo, prejudica a saúde financeira dessas.

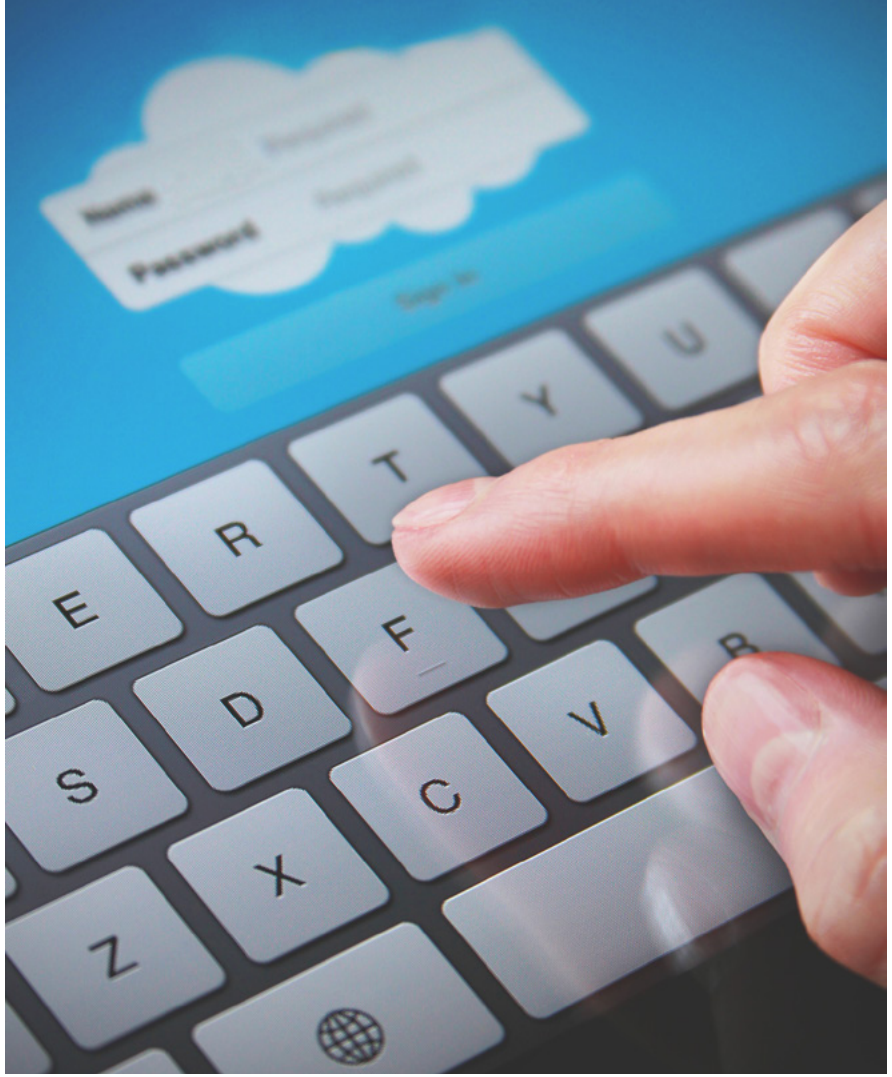
Além dos prejuízos diretos decorrentes dos ataques, há também os impactos financeiros devido a pausas nos escritórios ou linhas de produção até que os problemas sejam solucionados. Isso diminui a produtividade dos colaboradores, podendo atrasar entregas e até provocar problemas com clientes e fornecedores.

2. IMPACTOS NEGATIVOS NA IMAGEM E MORAL DA EMPRESA

A imagem e a moral da empresa junto ao mercado também podem ser seriamente comprometidas, gerando desconfiança por parte do público.

Afinal, uma ação criminosa virtual pode **expor inúmeros dados de funcionários, clientes e fornecedores de uma companhia**, afetando diferentes departamentos, como o de Recursos Humanos, o Comercial e o de Compras e Logística.

Por exemplo, em 2012 ocorreu um ataque ao LinkedIn, rede social voltada para profissionais e muito utilizada pelos RHs para processos de seleção e recrutamento mais eficazes. Na ocasião, cerca de 6,4 milhões de senhas foram divulgadas na web, comprometendo as contas e dados cadastrais de uma grande quantidade de usuários.



Hoje em dia, é cada vez mais comum que departamentos de RH conduzam processos seletivos em sistemas onlines, nos quais ficam armazenados dados sigilosos de candidatos e funcionários.

Significa que esses sistemas **também estão sujeitos a incursões cibercriminosas**, se não tiverem sido projetados considerando premissas de segurança da informação.

PROBLEMAS JURÍDICOS

Vazamentos de informações pessoais podem ocasionar uma **grande quantidade de processos judiciais** movidos por aqueles que tiveram seus dados expostos na web sem autorização.

Informações como senhas, dados de contatos, números de documentos ou valores de salários, nas mãos de criminosos, podem ser usados para roubo de identidade e trazer sérios problemas às pessoas lesadas, que responsabilizarão a organização pela ineficácia na guarda de dados sigilosos.

A segurança das informações precisa ser reforçada em empresas que trabalham com finanças e contabilidade, pois costumam interagir com uma gama ampla de dados sigilosos de pessoas e de outras empresas.

RETRABALHO DEVIDO À PERDA OU ROUBO DE DADOS

Quem já foi assaltado ou teve um bem furtado, sabe como é frustrante ter de recomeçar. Recuperar o patrimônio perdido causa desânimo e a sensação de retrocesso. A mesma sensação pode ser descrita com o retrabalho após o roubo de dados ou perda de arquivos.

Colaboradores têm de fazer o trabalho todo novamente, o que pode aumentar os níveis de estresse e diminuir o ânimo do grupo. A situação se agrava quando o incidente é recorrente e que poderia ser evitado se as tecnologias utilizadas não estivessem defasadas ou se fossem mais efetivas.

Como se proteger?

Agora que você já viu as principais modalidades de ataques, os riscos e os prejuízos causados, chegou a hora de descobrir o que você pode fazer para se prevenir contra eles.

Adiante, separamos **5 das principais atitudes que garantem maior proteção à empresa** no que diz respeito à segurança virtual. Confira:

1. USAR UM PACOTE COMPLETO DE SOFTWARES DE PROTEÇÃO

Utilizar um **bom antivírus** é uma medida básica para a sua empresa, porém, o número de ameaças se multiplicou nos últimos anos. Atualmente, recomenda-se ter um pacote mais completo capaz de prevenir a maior parte das ameaças virtuais.

É recomendado que ele contenha:

- antimalware;
- antiphishing;
- antispyware;
- antivírus;
- firewall efetivo;
- backup;
- antiadwares, entre outros.

Busque utilizar uma suíte de segurança de um fornecedor confiável, que contenha essas ferramentas, de modo a melhorar o desempenho da sua organização, deixando o ambiente de trabalho menos suscetível, aumentando a confiança dos colaboradores.

2. USO DE SOFTWARES NA NUVEM

Cloud Computing (**computação em nuvem**) é um conceito de arquitetura de TI que vem ganhando muita força nos últimos anos, impulsionando a criação de novos modelos de negócios, mais flexíveis e mais disponíveis para as empresas modernas.

Nessa arquitetura, empresas de tecnologia oferecem serviços de armazenamento e processamento de dados na web, como alternativa ao uso de recursos locais da sua empresa. Dessa forma, seus dados ficam guardados em ambientes virtuais otimizados, que são geridos por equipes especializadas em segurança da informação.

Utilizar serviços de nuvem traz as vantagens do acesso aos dados de qualquer lugar a qualquer hora, além de poupar você da gestão de equipamentos de hardware e de atualizações de software.

Algumas empresas oferecem sistemas de gestão na nuvem, de modo que não só seus arquivos, **mas também seus processos organizacionais ficam protegidos**. Isso inclui sistemas contábeis, sistemas de gestão financeira, de gestão de pessoas, entre outros.

3. REALIZAÇÃO DE BACKUPS CONSTANTES

A realização frequente de backups é uma medida básica que garante maior segurança para sua empresa, pois, além da perda de dados provocadas por ataques, imprevistos e panes podem ocorrer a qualquer momento. **Um sistema eficiente de backup pode lhe poupar tempo e dores de cabeça nesses casos.**

A possibilidade de recuperar seus dados, mesmo que se percam algumas horas de trabalho, pode até salvar o seu negócio da ruína.

O backup pode ser armazenado na nuvem, nesse caso, você tem maior proteção em situações de catástrofes, como em enchentes ou incêndios, que não só prejudicam os equipamentos, como também destroem os backups que foram guardados no local.

Os dados guardados em nuvem na verdade podem estar a quilômetros de distância da sua empresa, ou podem mesmo estar em outros continentes.

4. SELECIONAR FORNECEDORES CONFIÁVEIS

É essencial contar com software de qualidade, e fornecedores confiáveis que possuam boa reputação na hora de investir em soluções voltadas para a segurança da informação. Você dever contar com parceiros que possam fornecer apoio e suporte adequado em caso de necessidade.

5. CONSCIENTIZAÇÃO DE FUNCIONÁRIOS

Além de todas as medidas mencionadas para se proteger de incidentes e para lidar com as suas consequências, é importante conscientizar os colaboradores acerca de más práticas que podem sim furar todo o processo de segurança da empresa.

Abrir links suspeitos, espetar um pendrive de origem desconhecida e o uso de senhas fracas são alguns hábitos que podem abrir a porta para as ameaças, e que devem ser evitados no ambiente da organização.

Sempre use antivírus para varrer pen drives antes de acessar seu conteúdo e dispositivos.

Conclusão?

Como apresentado, **é importante que as empresas invistam em segurança da informação** para proteger seus fluxos de operações contra ataques externos, bem como prevenir ou diminuir o impacto causado por acidentes e descuidos, e garantir a continuidade do negócio.

Com o aumento incontestável do número de pessoas e organizações que passam a utilizar a web como meio para seus negócios e transações, a tendência é que o número de ataques virtuais também cresça em todo o globo. Novas formas de ciberataques devem surgir, e isso vai demandar a atualização constante das ferramentas de defesa e do nosso próprio comportamento na grande rede.

A escolha de bons parceiros de negócio comprometidos com a segurança da informação é fator importante para que a sua empresa possa pisar firme nesse novo mundo de conectividade sem fronteiras.

A **Fortes Tecnologia em Sistemas**, empresa do Grupo Fortes de Serviços, atua há mais de 25 anos na área de Tecnologia da Informação. Desenvolve soluções para gestão empresarial e abrange as seguintes áreas: gestão contábil, gestão financeira, gestão de pessoas e gestão de transporte e logística.

A empresa conta com uma carteira de milhares de clientes em todo o Brasil e uma rede de atendimento que inclui franquias e representações em vários estados das regiões Norte, Nordeste, Centro-Oeste e Sudeste.

O objetivo é oferecer um serviço dinâmico, moderno, de alto padrão e simples, sempre contando com a experiência de profissionais que entendem as necessidades dos negócios.

Quer saber mais como a **Fortes Tecnologia** pode ajudar?
Entre em contato conosco e conheça as soluções!

Eleito o melhor software contábil do Brasil.
Fonte: Pesquisa Nacional Nibo

www.**fortestecnologia**.com.br

CENTRAL DE VENDAS
0800 724 1110

/fortestecnologia @fortestec @fortes.tecnologia /FortesTecnologiaemSistemas

FORTES
tecnologia em sistemas