ECONOMIA

Cibercrime é ameaça a pequena empresa

Ataques virtuais às companhias brasileiras aumentaram 220% no primeiro semestre; grupos aprisionam dados em troca de resgate

PALAVRA DO EDITOR

A onda de ataques virtuais a gigantes corporativos ao redor do mundo faz com que as empresas precisem incluir a cibersegurança entre seus custos, assim como os seguros contra roubos nos moldes tradicionais.

ALVO GLOBAL

9,1
milhões
de ataques cibernéticos foram registrados no Brasil no primeiro semestre, segundo a consultoria Roland Berger

SANDRO THADEU
DA REDAÇÃO

Os ataques cibernéticos a empresas brasileiras cresceram 220% no primeiro semestre deste ano, em comparação ao mesmo período de 2020. O levantamento é do Grupo Mz e foi feito com base em dados apontados pela Comissão de Valores Mobiliários (CVM).

Esse dado e a divulgação de casos recentes de ações desse tipo envolvendo grandes marcas, como a Renner e a JBS, acenderam o sinal amarelo para a necessidade de se investir na proteção de dados.

Normalmente, os casos envolvendo grandes corporações ganham destaque na imprensa. Mas isso significa que muitos pequenos e médios empresários podem ficar despreocupados que seus negócios não serão alvo de hackers?

A resposta é não, segundo Dennis Riviello, o principal executivo da área de Cibersegurança da Compugraf, provedora de soluções de segurança da informação e privacidade de dados.

Segundo o especialista, um estudo recente, elaborado pelo Sebrae e pela Fundação Getúlio Vargas, aponta que as micro e pequenas empresas representam 30% do Produto Interno Bruto do Brasil (PIB). Por esse motivo, elas se tornaram alvo desses criminosos, que exploram as fragilidades dos sistemas e a falta de infraestrutura para agir.

"Todas as empresas estão no foco. Não há uma preferência. Óbvio que as grandes são mais suscetíveis a receber uma avalanche de ameaças, mas, pelo que estamos acompanhando nos últimos dois anos, há o crescimento exponencial das ameaças para pequenas e médias empresas", diz.

Por esse motivo, o especialista entende que é preciso ter um plano de ação ou preparo, caso ocorra uma tentativa de ataque. "Normalmente, o investimento é alto. Por isso, as empresas têm esse ponto sensível", afirma o assessor de investimentos Virgílio Lage.

Os principais ataques ocorrem por meio de um malware (software malicioso) conhecido como ransomware, um tipo de código que torna inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia.

Para que o usuário possa voltar a utilizar o sistema, os criminosos exigem das empresas o pagamento de resgate para desbloqueá-lo. Por esse motivo, Riviello aponta a necessidade de se injetar recursos para prevenir os cibercrimes.

"Esse investimento depende do tamanho da empresa, da quantidade de usuários e de outros fatores. É preciso fazer essa análise de riscos versus a perspectiva de ocorrer", disse.

IMPACTO NA CREDIBILIDADE

Os especialistas consultados por *A Tribuna* têm visões distintas sobre a repercussão negativa e o comprometimento da credibilidade das empresas que sofreram ataques cibernéticos.

"Elas podem perder valor competitivo no mercado. Afinal, é um risco de imagem e segurança muito alto que pode prejudicar clientes e fornecedores", justifica Lages.

Para Riviello, as consequências desses ataques dependem muito do nicho e do ramo de atividade. "Tivemos recentemente o caso da Renner e do Hospital Fleury, que não tiveram perda de credibilidade, porque investem muito nesse ambiente de segurança".

"O mais importante em uma situação dessa é o que a empresa faz para evitar esses ataques e como ela divulga isso, bem como os esforços que ela faz para minimizar os impactos aos colaboradores. Nesses dois casos, não vejo que perderam credibilidade ou clientes, mas tiveram impacto nas receitas por um breve período", completa.

CRIMINOSOS ON-LINE

O que é ransomware?
É um tipo de código malicioso que torna inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia, e que exige pagamento de resgate (ransom) para restabelecer o acesso ao usuário. O pagamento do resgate geralmente é feito via bitcoins

Como se propaga
Através de e-mails com o código malicioso em anexo ou que induzam o usuário a seguir um link

Explorando vulnerabilidades em sistemas que não tenham recebido as devidas atualizações de segurança

Tipos de ransomware
Ransomware Locker
Impede que você acesse o equipamento infectado

Ransomware Crypto
impede que você acesse aos dados armazenados no equipamento infectado, geralmente usando criptografia

Além de infectar o equipamento o ransomware também costuma buscar outros dispositivos conectados, locais ou em rede, e criptografá-los também

Como se proteger
Manter o sistema operacional e os programas instalados com todas as atualizações aplicadas

Ter um antivírus instalado

Ser cuidadoso ao clicar em links ou abrir arquivos

Fazer backups regularmente também é essencial para proteger os dados pois, se o equipamento for infectado, a única garantia de conseguir acessá-los novamente é possuir backups atualizados. O pagamento do resgate não garante que você conseguirá restabelecer o acesso aos dados.

Fonte: Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br)

INFOGRAFIA MONICA SOBRAL/AT

GIGANTES AMEAÇADAS

>>**Lojas Renner**
A varejista sofreu um ataque cibernético no dia 19 do mês passado. Essa ação dos criminosos afetou parte de sua operação. As operações no site foram restabelecidas dois dias depois. A companhia informou que não negociou ou fez o pagamento de resgate para recuperar seus sistemas.

>>**JBS no exterior**
Em junho deste ano, a maior empresa de carnes do mundo se viu obrigada a desembolsar a quantia de US$ 11 milhões (R$ 55,690 milhões) para solucionar um ataque hacker. Os invasores conseguiram desativar temporariamente as fábricas da companhia na Austrália, Canadá e Estados Unidos.

>>**Grupo Fleury**
A rede de laboratórios de diagnóstico médico foi alvo de um grupo de hackers intitulado REvil, no dia 22 de junho. Isso impediu que muitos pacientes tivessem acesso ao resultado de exames. A empresa demorou uma semana para conseguir restabelecer o acesso dos usuários ao sistema.

Funcionário pode ajudar a reduzir riscos

Em um mundo cada vez mais informatizado, a pandemia de covid-19 veio para consolidar algo que ainda era um tabu para muitas empresas brasileiras: o trabalho remoto.

Essa medida tornou-se uma necessidade para garantir a segurança sanitária dos funcionários e, ao mesmo tempo, assegurou uma importante economia de recursos para os empregadores com aluguel e outras despesas do dia a dia.

Além de investir nessa tendência, os especialistas em cibersegurança ouvidos por *A Tribuna* entendem que é necessário fazer um trabalho de conscientização dos funcionários para minimizar os riscos de ataques cibernéticos.

"As empresas devem investir em educação sobre tecnologia da informação e oferecer cursos e programas nesse sentido", afirma o assessor de investimentos Virgílio Lage.

O principal executivo da área de Cibersegurança da Compugraf, Denis Riviello, entende que a partir do momento que há soluções técnicas implementadas nos ambientes de trabalho e usuários bem treinados, os riscos de ataques são minimizados.

O especialista explica que é preciso deixar claro que os funcionários sejam orientados a não abrir arquivos de fontes duvidosas, links maliciosos e sites desconhecidos.

"Se você tem ferramentas por trás para inibir esse tipo de ação, você tem menos êxito em uma possível contaminação. Um usuário bem instruído e bem conscientizado está menos suscetível a fazer uma ação que venha trazer algum prejuízo à empresa", destaca.