MÚLTIPLAS VOZES

Cibercriminalidade: estratégias e perspectivas para enfrentar esse delito

A segurança cibernética não é responsabilidade apenas de especialistas, pois ela afeta a todos que trabalham no setor público e os próprios cidadãos

José Mariano de Araujo Filho
9 de dezembro de 2020

MARCELLO CASAL JR / AGÊNCIA BRASIL

Ataque ao sistema de informática do STJ impediu acesso a dados do tribunal por vários dias

Recentemente, a população brasileira foi surpreendida com informações que davam conta de um ataque cibernético aos sistemas informatizados do Superior Tribunal de Justiça, o que inviabilizou o acesso aos dados daquela corte por vários dias.

Esta notícia poderia passar desapercebida diante da quantidade de ciberataques dos quais são alvos corporações privadas e públicas nos dias atuais, mas acabou por se sobressair aos casos rotineiros por conta do potencial ofensivo do ataque praticado pelos criminosos responsáveis.

Embora nenhuma organização esteja imune a uma violação de dados, o setor público está particularmente vulnerável, especialmente à medida que mais serviços aos cidadãos ficam online.

Fato é que a “digitalização” do setor público também não escapou à atenção dos cibercriminosos, que agora desejam lucrar roubando grandes quantidades de dados valiosos que residem nessas organizações.

Infelizmente, casos como o do STJ não são um incidente isolado, apenas ocorreu uma publicidade maior de seu alcance e as suas consequências alcançaram uma divulgação bem mais ampla.

Apesar do perigo claro e presente e com o crime cibernético começando a ocupar um lugar mais alto na agenda do governo, especialmente à luz de uma maior publicidade de incidentes na esfera pública, o setor ainda não consegue compreender a escala da ameaça bem à sua porta.

Para organizações do setor público em particular, é fundamental que mantenham um controle estrito sobre seus dados, devido à natureza altamente confidencial das informações com as quais lidam.

As implicações de não fazer isso também colocam os cidadãos em risco - especialmente se as informações furtadas consistirem não apenas em nomes de usuário e senha.

Fato é que as organizações públicas necessitam entender o que é preciso para navegar no cenário de segurança cada vez mais vulnerável de hoje.

Mas a pergunta que não quer se calar é, quais medidas o setor público pode tomar para se proteger do risco crescente de crimes cibernéticos?

A segurança cibernética não é responsabilidade apenas de especialistas em tecnologia da informação, pois a mesma afeta a todos os que trabalham no setor público, junto com os próprios cidadãos, então isso deveria estar na mente de todos dentro de uma organização.

No entanto, muitas vezes, a responsabilidade pela segurança começa e termina com a contratação de “empresas especializadas”, o que significa que esses incidentes continuarão a ocorrer, pois ou a equipe de gerenciamento sênior ignora a importância de uma boa higiene de segurança ou os profissionais de segurança da informação estão falhando em comunicar a mensagem.

Gestores públicos e privados devem garantir que a educação em segurança cibernética e o treinamento de conscientização sejam realizados regularmente, pois ao fazer isto os funcionários estarão mais propensos a se comportar de uma forma que evite o vazamento de dados.

O cenário de ameaças cibernéticas está em constante mudança, por isso é de suma importância para as organizações públicas e privadas se manterem atualizadas com os desenvolvimentos mais recentes em segurança cibernética.

Quaisquer novos riscos de segurança, por menores que pareçam, devem ser comunicados a todas as organizações para que os envolvidos entendam o que procurar e quais são as melhores práticas para prevenir esses riscos.

Além disso, cibersegurança deve ser uma iniciativa apoiada e incorporada pelo governo, a qual visa fornecer orientações e conselhos mais claros para organizações que buscam melhorar a manutenção da segurança cibernética.

Este tipo de inciativa é voltada para aqueles que podem não ter uma equipe de tecnologia da informação interna dedicada e responsável pela segurança cibernética.

Embora a maioria dos departamentos do setor público tenham isso em maior ou menor grau, é indispensável e valioso o fornecimento de bases sólidas para instituições públicas e privadas, visando a melhoria das práticas de segurança.

Também é imprescindível e necessário que a administração pública adote uma postura proativa, a qual lhe permita não apenas reagir aos ciberataques visando majorar os seus efeitos, como também criar uma política pública que privilegie a investigação de todos os incidentes.

Incutir uma mentalidade de segurança em toda as organizações pública e privadas, por meio do treinamento, é a primeira metade da batalha.

Mas é necessário e vital que as organizações avancem mais na investigação e repressão dos incidentes de segurança.

Se o setor público deseja realmente obter os benefícios de se tornar digital, ele deve permanecer constantemente à frente dos criminosos cibernéticos, implementando novas soluções de tecnologias que sejam capazes de combater as táticas cada vez mais avançadas dos criminosos, inclusive com a identificação dos mesmos e a sua submissão à Justiça.

As organizações do setor público devem trabalhar em estreita colaboração com corporação privadas para adotar novas ferramentas e práticas que ofereçam o máximo de resiliência contra ameaças.

A título de exemplo, a tecnologia biométrica, quando combinada com tecnologia para eliminar senhas, é um meio alternativo de autenticação, ao contrário das senhas tradicionais, e torna mais fácil para as organizações determinarem exatamente quem está acessando um sistema ou aplicativo.

Como essa tecnologia é única para cada indivíduo, a autenticação biométrica cria responsabilidade; cada transação ou ação é documentada junto com o indivíduo associado a ela.

Continuar a usar a tecnologia de senha é quase como colocar uma placa na porta da frente informando a qualquer um que a chave da casa está escondida debaixo do tapete!

Já é passada a hora das empresas públicas e privadas colocarem suas casas em ordem, já que a ameaça real que as mesmas enfrentam não é apenas quanto uma violação cibernética vai custar, mas o custo de ter que contar para todos, algo muito mais crucial neste momento em que a Lei Geral de Proteção de Dados torna compulsória informações de vazamentos de dados.

O Brasil não tem qualquer tipo de estatística que apresente informações mínimas para a criação de uma estratégia efetiva de combate aos cibercriminosos, o que impede até mesmo um planejamento mais eficiente e a repressão adequada das ameaças.

Em última análise, a prevenção do crime cibernético tem tanto a ver com mudança cultural quanto com soluções tecnológicas e investigação de incidentes.

Por fim, é importante destacarmos que países com maior controle governamental sobre a infraestrutura crítica e também sobre sua infraestrutura de informação têm potencialmente uma vantagem significativa no combate às ciberameaças, uma vez que eles são capazes de controlar e moldar sua resposta à insegurança cibernética com maior autonomia.

É possível que uma abordagem liderada apenas pelo segmento privado para a segurança cibernética nacional provará ser menos eficaz do que uma abordagem liderada pela administração pública.

Também é possível ser necessário repensar a amplitude e a profundidade da segurança da informação, na qual podemos anexar de forma útil todas as expectativas da segurança cibernética nacional, inclusive reconhecendo a incapacidade de uma abordagem mais efetiva de nossas estratégias, pois é essencial para o desenvolvimento do país uma ação robusta e proativa para a segurança do estado na era da informação.

Os dados são um dos ativos mais valiosos que uma organização possui, portanto, as soluções de segurança utilizadas para proteger essas informações devem se adaptar.

Ao mesmo tempo, todos em uma organização devem tratar o crime cibernético da mesma forma que tratariam a segurança física. O futuro de qualquer organização que queira se isolar da crescente ameaça do crime cibernético depende disso.

José Mariano de Araujo Filho
Delegado de Polícia, especialista na investigação de cibercrimes e professor da Academia de Polícia Civil de São Paulo

---

https://www.fontesegura.org.br/multiplas-vozes/p57gereagu