Segurança online – 5 erros comuns que as empresas praticam

As empresas devem estar atualizadas para evitar o risco de quebras de informação. Tanto pelo crescimento a pique dos ataques online como dos contantes erros que se pratica no mundo digital.

As entidades encontram, agora, dois caminhos que devem ser percorridos lado a lado: o caminho da transformação digital, para obterem um avanço competitivo, e o caminho da segurança dos seus dados.

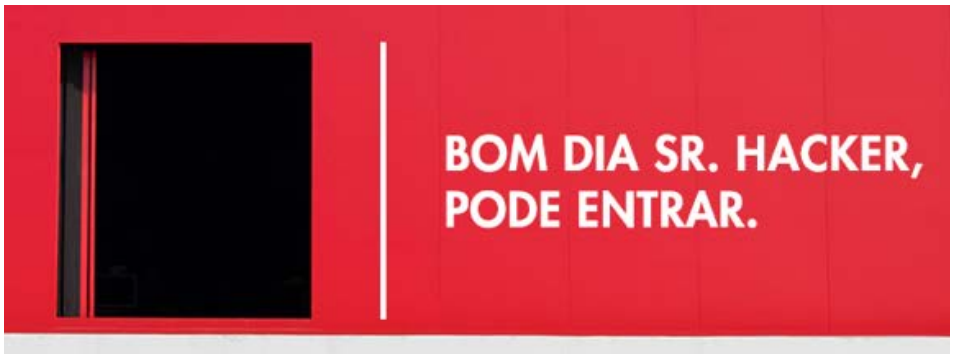
Enfrentando os ataques, só fará a sua empresa ficar mais forte. O Departamento de Engenharia de Sistemas da Samsys explica-lhe 5 erros comuns que acontecem nas empresas:

1. Não praticam uma higiene básica dos seus sistemas

Os ataques sofrem alterações e com o avanço da tecnologia tudo é possível. A maioria das empresas tem nas suas instalações sistemas complexos de redes com imensas oportunidades para os hackers se infiltrarem e conseguirem quebrar a sua segurança. Aquilo que denominamos "falta de higiene de rede básica", como software desatualizado e sistemas operacionais não adequados, coloca a sua empresa em risco de ataque.

2. Confiar em vários fornecedores de terceiros

Algumas das empresas mais avançadas do mercado já perceberam que devem alinhar a sua estratégia de segurança para proteger o maior ativo das suas organizações: os dados. Atualmente as empresas tendem a trabalhar com muitos fornecedores de terceiros que desenvolvem aplicações ou fornecem serviços. Sabe o poder que esses prestadores de serviços têm na sua empresa? Será que têm 100% de acesso aos seus dados?



3. Acreditam que um antivírus é suficiente

Confiar exclusivamente a segurança da sua empresa a um simples antivírus é um erro bastante comum e arriscado. O crime informático está, apenas, a um e-mail pishing bem-sucedido de acontecer: um clique num link e os dados da sua empresa deixam de ser seus.

4. Não criam uma cultura de segurança online

Embora muitos dos ataques online que acontecem sejam a grandes empresas, é errado criar a premissa que todos os outros negócios não sejam ou vão ser alvo de um ataque. A melhor maneira de evitar é prevenir. Ou seja, criar uma cultura de consciencialização de segurança online. Todos os colaboradores devem estar conscientes das ameaças existentes e evitar que as ameaças se concretizem em realidade.

5. Não se preparam para um eventual ataque

As empresas devem aceitar o facto de este tipo de situações não acontecer só às outras. A chave é ter um plano que permita prevenir ou recuperar de uma eventual quebra no sistema. ■