

Coronavírus x ambiente cibernético: você sabe como proteger sua empresa?

Escrito por: Horiens - 13/04/2020

Do mundo físico para o virtual num estalar de dedos. Sim, a covid-19 fez os cyber risks dispararem a luz vermelha nas agendas das empresas. Se os ciberataques já eram considerados um dos grandes riscos da atualidade, agora a situação ficou consideravelmente mais crítica.

No Brasil, a quantidade de dispositivos digitais em uso já supera o número de brasileiros. Some-se a isso o aumento do volume de informações estratégicas que circula na rede, em tempos de quarentena para prevenção ao coronavírus e, conseqüentemente, home office. Tudo isso cria um cenário de maior vulnerabilidade que é um prato cheio para crimes virtuais, dos mais variados tipos e proporções.

“A necessidade de que as empresas adotem uma forte estratégia de segurança da informação digital nunca foi tão grande como agora”, explica Eduardo Damião, especialista em Seguros de Riscos Cibernéticos da Horiens.

A dimensão do problema

Já sabemos que bem antes do novo coronavírus, os cyber risks tinham lugar cativo na lista dos grandes riscos do século. Para se ter uma breve ideia, o Internet Crime Report, do FBI, consolidou dados de 2019 referentes a mais de 400 mil denúncias de todo o mundo, que somaram mais de US\$ 3,5 bilhões de prejuízo às vítimas.

O Brasil é um alvo importante dos ciberataques. Um estudo da Symantec mostra que o país está entre os principais alvos e é o 4º no ranking de crimes cibernéticos, atrás apenas dos Estados Unidos, China e Índia.

Em meio à crise atual, um relatório do Fórum Econômico Mundial, divulgado no último mês de março, inclui os ataques cibernéticos entre os riscos que podem trazer impactos negativos em vários setores pelo período de 10 anos. De acordo com o relatório, 75% dos cerca de 750 especialistas e líderes consultados esperam um aumento nos ataques em busca de dados ou dinheiro no atual cenário.

Outro estudo, da Apura Intelligence, consultoria brasileira especializada em segurança digital, divulgou dados que contabilizam mais de 63 mil eventos potencialmente fraudulentos mencionando a palavra coronavírus no Brasil.

Como se vê, dados não faltam para alertar a potencialização dos cyber risks.

Mas quais são os riscos cibernéticos mais recorrentes?

Estamos falando de situações que envolvem desde roubo de dados a invasões e sabotagem de sistemas de infraestrutura, energia e abastecimento ou ainda financeiros, por exemplo, com potencial de causar efeitos impactantes para a sociedade e a economia em geral. As conseqüências podem ser localizadas ou de proporções gigantescas. Todas, de alguma forma,

trazem prejuízo.

De acordo com dados do Internet Crime Report, do FBI – relatório citado acima –, cerca de metade das perdas computadas em 2019 ocorreu por fraudes do tipo Business E-mail Compromise (BEC), quando o golpista engana funcionários de uma empresa por meio de mensagens de e-mail para que pagamentos sejam realizados em contas controladas por hackers. Há modalidades mais avançadas deste tipo de golpe, com invasões à rede de uma empresa para buscar informações de pagamentos e fornecedores.

Em 2020, o combate ao coronavírus acabou criando o ambiente ideal para o ataque de hackers. Arquivos disfarçados que se utilizam do nome coronavírus estão espalhados pela rede – mas não se engane e tome cuidado – muitas vezes o objetivo destes arquivos é danificar ou criptografar dados.

Entre os crimes cibernéticos mais comuns, tanto para usuários quanto para empresas, destacam-se os chamados **DDoS**, ataques de negação de serviço realizados por meio de sobrecarga nos servidores das empresas, tirando serviços do ar. Este formato de crime tem impacto direto nas operações, causando prejuízos financeiros. Mas os problemas não param por aí, muitas vezes esse tipo de crime é uma distração planejada para tirar o foco da segurança de TI e abrir território para a aplicação de golpes mais elaborados.

A lista de possíveis crimes ainda inclui **sequestro de dados (ransomware), invasão de sistemas, instalação de vulnerabilidades, vazamento de dados ou conteúdo pessoal, comprometimento de sistemas de segurança**, entre outros.

E-mails disfarçados com remetente desconhecido ou bots, os chamados robôs de internet, são exemplos de estratégias utilizadas pelos hackers para cometer os cibercrimes.

Como se proteger?

Especialistas mostram que a questão não é “se” a empresa sofrerá um ataque cibernético, mas sim, “quando”. Na era da informação em que vivemos, é necessário se debruçar sobre o tema, entender o risco e suas consequências, de ponta a ponta.

Isso inclui ações como atualizar constantemente os sistemas de tecnologia, revisar periodicamente a política de segurança digital da empresa, campanhas educativas para funcionários e contratação de seguros específicos, por exemplo.

“A demanda pelas apólices de cyber risks está maior. As empresas precisam avaliar a sua exposição em primeiro lugar para então transferir parte destes riscos para uma apólice de seguro que melhor atenda às suas necessidades. Mesmo não transferindo todos os riscos, por meio do seguro há a mitigação dos possíveis danos/reclamações. O tema requer atenção e ação por parte das empresas”, conclui Eduardo Damião.