O cibercrime não está de quarentena

dinheirovivo.pt/opiniao/o-cibercrime-nao-esta-de-quarentena-12689647.html

30 de março de 2020

O cibercrime não está de quarentena. Pelo contrário, encontra-se em plena atividade! Tem, até, encontrado um terreno bastante fértil para crescer, neste que é o novo "escritório" de grande parte da população mundial: o ciberespaço.

Aliás, o cibercrime é tão imune à pandemia que chega mesmo a servir-se dela para atacar, com cada vez mais sucesso, indivíduos e organizações, em particular, aquelas que não estavam suficientemente preparadas para o teletrabalho.

Aquilo que temos vindo a defender, há muito, ganha agora uma nova dimensão:

-- A continuidade dos prestadores de serviços essenciais, sejam eles serviços de comunicações, saúde, segurança ou bens de primeira necessidade, não pode estar à mercê de ciberataques, como os que a Organização Mundial de Saúde (OMS) ou alguns hospitais espanhóis têm sofrido nos últimos dias;

-- A continuidade dos negócios depende, mais do que nunca, da implementação de medidas de cibersegurança. Muitas empresas, respondendo aos desafios da presente pandemia, passaram a sua atividade para um estado (quase exclusivamente) *online*, completamente dependente das comunicações e segurança instituídas singularmente – em modo *home made* - pelos seus próprios colaboradores, sem, obviamente, estarem preparadas para as "normais" exigências da sua atividade ou negócio;

-- A formação de todos os colaboradores para a segurança da informação – e não apenas da camada decisora das empresas ou dos técnicos de informática – tem de ser um requisito, sobretudo agora que a grande maioria se encontra a trabalhar de casa, sem as garantias de segurança habituais providenciadas pela estrutura corporativa.

As ferramentas de suporte ao teletrabalho como o Skype, o Teams ou o Zoom substituem as habituais salas de reunião ou visitas ao cliente, mas quais as mais adequadas à minha organização?

O correio eletrónico continua a ser fundamental e vem, agora, reforçar o seu papel na comunicação dentro e fora das organizações, mas como assegurar o seu bom funcionamento e ensinar os meus colaboradores a distinguir ataques de *phishing* de *e-mails* legítimos?

E as tradicionais políticas de cópias de segurança, atualização regular de *software* ou alteração de passwords mantêm-se?

Estas são apenas algumas das muitas questões com as quais temos sido confrontados nas últimas semanas e a resposta às mesmas… varia.

Se, em termos gerais, é necessário aumentar drasticamente o nível de segurança em volta da "nossa casa" e incrementar os nossos sentidos de vigilância de tudo o que sentirmos como "cibernauticamente" suspeito, é preciso também ter consciência de que cada caso é um caso e cada negócio é um negócio.

A dimensão da empresa, quer em número de recursos quer em geografia (local, nacional, internacional), a sua capacidade e evolução tecnológica, a estrutura de suporte, a sensibilidade dos colaboradores para estas matérias, a experiência em trabalho remoto, e, sobretudo, o grau de maturidade em termos de segurança da informação vão afetar as necessidades das organizações, podendo, muitas vezes, implicar soluções diferentes para organizações aparentemente semelhantes.

Além disso, face aos desafios da atual conjuntura económica, que são de incerteza e adversidade, em que é preciso priorizar a operação e manutenção do negócio, sabemos que nem sempre a solução ideal é possível. Mas isto não significa descurar a cibersegurança. Pelo contrário, significa geri-la da melhor forma, garantido que se trata de mais um incremento na proteção do negócio e viabilidade das empresas enquanto não ultrapassamos este tsunami pandémico.

Temos de reverter a tendência de olhar a cibersegurança como um extra ou um luxo de alguns, pois são esses alguns que acabam por conseguir reagir com sucesso aos desafios do presente.

Afinal, como temos aprendido da pior forma, a segurança – e, assim, a cibersegurança – é basilar.

O mundo não está a mudar, o mundo mudou. E, por isso, também nós temos de mudar.

Bruno Castro é CEO da Visionware