Como é que as empresas podem evitar ciberataques durante a pandemia

jornaleconomico.sapo.pt/noticias/como-e-que-as-empresas-podem-evitar-ciberataques-durante-a-pandemia-579591

23 de abril de 2020

O cibercrime aumentou durante esta crise pandémica e está a impactar consumidores e empresas portuguesas, que se deparam quer com ataques de *ransomware* quer com *phising*, através de emails e aplicações maliciosas como a Covid-19 Tracker. Aliás, o Centro Nacional de Cibersegurança identificou uma subida no número de ataques cibernéticos no último mês, contabilizando mais de 100 incidentes ao longo do mês passado e na primeira quinzena de abril.

A empresa de segurança informática VisionWare diz que o novo coronavírus tem funcionado como um "isco" para os *hackers*, que se fazem passar por entidades de renome ou autoridades de saúde oficiais, como a Organização Mundial de Saúde.

O CEO, que é um dos auditores credenciados pelo Gabinete Nacional de Segurança, considera que, neste momento, todos os setores estão vulneráveis a estes 'piratas digitais', mas é necessário que os prestadores de serviços essenciais (comunicação, saúde ou bens de primeira necessidade) estejam mais atentos, porque qualquer falha pode pôr em causa o funcionamento e a estabilidade do país.

"Os ataques de *ransomware*, tendência que já vinha a crescer nos últimos anos, assim como os de DDoS [ataques de negação de serviço], também têm sido particularmente bem sucedidos, tendo já sido reportados casos de tentativa de interrupção dos serviços

informáticos de infraestruturas críticas como operadores de comunicação, governamentais ou serviços essenciais, como por exemplo hospitais em Espanha", refere Bruno Castro.

À parte esses esquemas, existem outras circunstâncias que podem trazer à tona mais problemas: as notícias falsas e publicações falsas que circulam, a utilização de métodos de pagamentos digitais e de aplicações colaborativas pouco seguras, o aumento do tráfego de internet e o uso de computadores pessoais desprotegidos para o teletrabalho.

"Um acesso remoto (VPN) mal configurado pode expor uma organização aos riscos/ameaças de segurança das várias redes "caseiras" dos seus colaboradores, basta imaginar a ameaça que pode advir das famílias dos colaboradores no acesso "descontrolado" existente numa rede caseira (P2P, vírus, *ransomware*, entre outros)", exemplifica o diretor e sócio da VisionWare.

No ano passado, a Autoridade Nacional de Comunicações (Anacom) registou 80 incidentes de segurança comunicados pelas empresas de redes e serviços de comunicações eletrónicas em 2019, menos 29% do que no ano anterior, mas essas oito dezenas foram mais gravosas – i.e. afetaram mais assinantes ou acessos.

Para evitar riscos cibernéticos, esta empresa portuguesa de cibersegurança tem cinco conselhos para as organizações:

- Implementar medidas ativas de segurança com um nível mais exigente face à necessidade de dar acesso remoto aos trabalhadores através das suas redes domésticas.
- Capacitar os colaboradores para o acesso aos sistemas corporativas de forma a permitir o seu trabalho "normal" e protegerem-se face às ameaças que advêm desse mesmo acesso. Ou seja, as empresas têm que se proteger dos "colaboradores", e simultaneamente, dar ferramentas que permitam dar maior segurança aos colaboradores enquanto estão em teletrabalho nas suas casas.
- Implementar sistemas de monitorização e alarmística de segurança que possa detetar alguma atividade suspeita na rede corporativa;
- Formar os colaboradores
- Recorrer à consultoria para ajudar a definir prioridades e a escolher o melhor modelo de teletrabalho, nas vertentes de segurança e de qualidade de serviço prestado.