

Por Alexandre Finelli

Diversos estudos mostram que as empresas levam algumas centenas de dias para descobrirem que foram atacadas. Se este número já é capaz de causar arrepios em qualquer CEO preocupado com a segurança de sua organização, imagine se ele soubesse que a investigação de um crime pode levar até um ano para ser desvendado. Pois é esse o prazo médio que uma ocorrência virtual leva para ser decifrada no Brasil.

Segundo Emerson Wendt, delegado de Polícia especialista em investigação de crimes cibernéticos, a média de apuração de delitos informáticos é maior, porque há uma fase técnica de análise de dados, de entender a prática da ação ilícita e, com base nisso, estabelecer as próximas estratégias. “Também é preciso contar com o apoio de provedores e servidores, o que demanda mais tempo. Dependendo do caso e da complexidade, uma investigação leva até sete meses. Quando é preciso cooperação internacional, a média é entre nove e 12 meses”, afirma.

Desafios

Wendt relata que obter dados de provedores de aplicações internacionais atrasa bastante a investigação, já que alguns rejeitam as ordens judiciais brasileiras. Quando se trata de conteúdo, por exemplo, muitas interpretam uma ação como direito à liberdade de expressão. Porém, se há suspeita de fraude, algumas fornecem dados cadastrais e logs de acesso.

Além disso, acrescenta-se o fato de o Brasil enfrentar grandes problemas de estrutura e processos. “É preciso qualificar melhor os policiais, juízes, promotores e advogados para compreenderem o funcionamento, a terminologia e a tecnologia em si para realizarem um trabalho mais bem feito”, sugere. Em sua opinião, falta mais conhecimento técnico e científico dos envolvidos nas práticas investigativas. “Se você quer apurar um crime de internet precisa dominar a plataforma pela qual aconteceu o ato”.

Organizações sob risco

Entre os crimes mais difíceis de serem investigados estão os ataques de negação de serviço (DDoS) e o Ransomware, tipo de malware que restringe o acesso ao sistema infectado e cobra um valor de “resgate” para o acesso ser restabelecido. “O primeiro por ser um ataque que vem de vários locais ao mesmo tempo, com programação remota, sendo bastante complexo de analisar. O segundo pela dificuldade de quebrar a criptografia”, explica. O especialista afirma que não conhece casos recentes de alguém que tenha conseguido quebrar o código, senão mediante pagamento do resgate.

O que chama a atenção, segundo Wendt, é o crescimento de ataques do tipo Ransomware no mundo, inclusive, no Brasil. Isso mostra o quanto as organizações estão ignorando itens básicos de Segurança da Informação, como backups constantes. O especialista afirma que se uma organização realizasse backup a cada 24 horas ou semanalmente, o que é esperado de uma empresa de grande ou médio porte, o prejuízo seria mínimo e mais fácil de ser recuperado.

Isso quer dizer que, se as empresas estivessem fazendo a lição de casa, sem dúvida, essa prática seria abolida ou, no mínimo, reduzida drasticamente. “Geralmente, paga-se quando não se tem o backup, ou seja, se há educação prévia e compliance, isso possivelmente seria eliminado”, finaliza.

Fonte: [Risk Report](#), em 20.08.2015.