Relatório da BT e da KPMG adverte sobre ameaças emergentes que têm origem em organizações cibercriminosas altamente organizadas

Apenas um quinto dos executivos de TI das grandes empresas multinacionais afirma que suas organizações estão realmente preparadas para combater a ameaça do cibercrime. A grande maioria das companhias se sente limitada por regulamentações, disponibilidade de recursos e a dependência de terceiros quando se trata de reagir a esses ataques.

Segundo pesquisa da BT e da KPMG, intitulada "Taking the Offensive – Working Together to disrupt digital crime", embora 94% dos responsáveis pelas decisões em TI estejam cientes de que esses "empresários criminosos" chantageiam e subornam funcionários para ter acesso a suas organizações, cerca de metade deles (47%) admite que suas empresas não implementa qualquer estratégia para impedir essas ações.

O estudo também verificou que 97% dos entrevistados já foram alvo de ataques cibernéticos, que, segundo metade deles, vêm se intensificando nos últimos dois anos. Além disso, 91% acreditam que enfrentam obstáculos em suas defesas contra os ataques digitais: muitos deles citam entraves regulatórios, e 44% se mostram preocupados com a dependência de terceiros para ações de resposta que são de sua responsabilidade.

Mark Hughes, CEO da área de segurança da BT, destaca que "estamos agora em uma corrida armamentista contra gangues de criminosos profissionais e contra estados que possuem recursos avançados. No século 21, os cibercriminosos são empresários cruéis e eficientes, atuando em um mercado negro altamente sofisticado e em rápida evolução.

"A contínua escalada do cibercrime exige uma nova abordagem em relação ao risco digital – e isso significa, em primeiro lugar, colocar-se na pele dos atacantes. Não basta as empresas se defenderem dos ataques. É preciso também interromper as atividades das organizações criminosas que lançam esses ataques. As empresas precisam contar com leis aplicadas contra os criminosos, e também com a competência de parceiros especializados em segurança cibernética".

Paul Taylor, que está à frente da área de segurança cibernética da KPMG no Reino Unido, ressalta que "é tempo de pensar o risco cibernético sob outro ângulo, retirando o foco exclusivamente dos hackers, e reconhecendo que nossas organizações estão sendo alvo de empresários criminosos e impiedosos, que têm planos de negócio e utilizam amplos recursos com intenção de fraudar, extorquir e roubar a propriedade intelectual do que lutamos para conquistar.

"Falar de forma genérica sobre o risco digital não vai apresentar soluções. É necessário pensar em possíveis cenários de ataque à sua empresa e considerar como a segurança cibernética, controle de fraude e resiliência podem ser combinados para lidar com essas ameaças de modo eficiente. Dessa forma, a segurança cibernética se torna uma estratégia corporativa importante para os negócios no mundo digital".

O estudo da BT/KPMG indica que os Chief Digital Risk Officers (CDROs) agora estão sendo chamados a assumir um papel estratégico, somando experiência no mundo digital e competência gerencial de alto nível. Entre os entrevistados, 26% disseram já contar com um profissional nessa função, o que sugere que a área de segurança e as responsabilidades inerentes a ela estão sendo reavaliadas.

A pesquisa também sinaliza a necessidade de ajuste dos orçamentos, e 60% dos entrevistados indicaram que, nas suas empresas, a segurança cibernética faz parte do orçamento de TI. Metade deles (50%) acredita que deveria haver um orçamento específico para segurança. Um dos maiores desafios identificados pelo relatório é o volume de financiamento e investimentos em P&D que os criminosos conseguem reunir para minar as defesas das empresas alvo.

A pesquisa relata, também, exemplos de diversas formas de ataques criminosos identificados por essas organizações, incluindo diferentes tipos de malware e ataques de phishing. Também descreve os principais modelos de negócio dos criminosos e o mercado negro que permeia suas atividades – sejam sofisticados ataques ao sistema financeiro; ataques a empresas ou indivíduos com alta renda, ou até mesmo ataques que já se tornaram commodities, afetando a todos nós.

As conclusões apontam para a necessidade de uma nova mentalidade, considerando a segurança não mais apenas como um exercício de defesa. A segurança, na verdade, é ponto crucial para a inovação digital e, em última instância, para a lucratividade das empresas.

Fonte: Computerworld, em 06.07.2016.