CrowdStrike: interpretar a falha que impactou o mundo

digitalinside.pt/crowdstrike-interpretar-a-falha-que-impactou-o-mundo

Atualmente, a infraestrutura digital é o alicerce de quase todas as atividades diárias, desde transações financeiras e comunicação, até serviços públicos essenciais chegando até à segurança nacional. Esta conectividade digital, embora traga inegáveis benefícios, expõe também a sociedade a vulnerabilidades significativas que podem ter consequências desastrosas chegando ao extremo de comprometer o estado de direito de uma nação. Qualquer interrupção pode resultar em perdas financeiras substanciais e comprometer desde o tecido empresarial, às instituições de cariz público até às pessoas como indivíduos que dependem do mundo digital para "viver". Um dos exemplos mais expressivos talvez seja o das infraestruturas de saúde, que dependem de registos eletrónicos de pacientes e sistemas de telemedicina e que, por esse motivo, enfrentam graves consequências em caso de falhas tecnológicas. A interrupção desses sistemas pode atrasar diagnósticos, tratamentos e até mesmo colocar vidas em risco. A segurança dessas infraestruturas é vital para o funcionamento diário da sociedade e sua vulnerabilidade tecnológica é uma preocupação crescente. Além dos impactos diretos, uma falha tecnológica de grande dimensão, como foi o caso, pode abalar a confiança da sociedade nas instituições de saúde e em toda a estratégia de digitalização em curso no panorama da administração pública.

O desastre tecnológico ocorrido, com a dimensão do impacto a nível mundial, veio ainda colocar em maior evidência, a urgência de implementar critérios mais rigorosos de segurança e controlo para fabricantes de software de segurança. Este é um exemplo não apenas de alerta sobre as vulnerabilidades inerentes aos sistemas de segurança, mas também vem reforçar a necessidade imperativa de uma revisão e fortalecimento das práticas regulatórias e de auditoria para os fornecedores de soluções de segurança digital. A CrowdStrike, uma das empresas mais respeitadas no setor de segurança, e a Microsoft, gigante da tecnologia, foram vítimas de uma falha que comprometeu a segurança de inúmeros sistemas pelo mundo todo. A ironia de uma empresa de segurança ter sofrido uma falha tão significativa não pode ser subestimada – levantam-se questões críticas sobre a eficácia das medidas de segurança implementadas por essas empresas e, mais importante, sobre a confiança que os consumidores e outras empresas depositam nas mesmas. Era suposto que um fabricante de soluções de segurança implementasse os mecanismos mais exigentes de controlo de qualidade antes de "libertar" as novas versões para o mundo inteiro. Essa perceção, mais ou menos consensual, de que os fabricantes de segurança são mais "confiáveis" que o resto da comunidade de fabricantes, tornou-se, agora, mais discutível.

A primeira questão que deve ser abordada é a transparência. Empresas de segurança lidam com informações altamente sensíveis e a confiança é um pilar fundamental do seu relacionamento com os seus clientes. Falhas como esta minam essa confiança e sugerem que a transparência é essencial não apenas na comunicação de falhas, como também nos processos internos de desenvolvimento, controlo de qualidade e

posteriormente, na disponibilização das atualizações das suas próprias soluções de segurança junto da sua comunidade de clientes. Além da transparência, a regulamentação precisa ser reforçada. Atualmente, as regulamentações de cibersegurança variam amplamente entre diferentes jurisdições, o que pode, por vezes, causar conflitos ou fragmentação. Uma abordagem mais harmonizada e robusta é necessária, onde os fabricantes de segurança sejam submetidos a um conjunto consistente de normas e requisitos de conformidade tal como seria outro qualquer fornecedor aplicacional ou fabricante tecnológico.

Outra dimensão crucial para tal reforço e ações de cooperação, diz respeito à colaboração entre fabricantes de segurança, governos e outras partes interessadas. A partilha de informações sobre vulnerabilidades em tempo real pode ajudar a mitigar riscos antes que estes se tornem críticos e altamente prejudiciais.

A cibersegurança não pode ser tratada de forma negligente, especialmente, por aqueles que prometem proteger outros de ameaças digitais. A confiança no mundo digital depende disso e as empresas de segurança devem ser implacáveis em garantir que tais falhas não se repitam voltando a tornar-se o principal exemplo de exigência no cumprimento das boas práticas do setor. Fica claro que o mercado passou, agora, a desconfiar também das empresas e fabricantes de segurança.

Bruno Castro é Fundador & CEO da VisionWare. Especialista em Cibersegurança e Investigação Forense.