

O número crescente de incidentes de segurança mostra lacunas de comunicação entre ferramentas e o baixo nível de automação

É uma mistura explosiva: embora o número de incidentes de segurança continue a aumentar, muitos dos departamentos de segurança das seguradoras brasileiras carecem de mão de obra e automação para acompanhar. Mais da metade dos entrevistados brasileiros da pesquisa "[OTRS Spotlight: Corporate Security 2023](#)" relatam um leve aumento (52%) ou acentuado (20%) nos incidentes nos últimos doze meses. Ao mesmo tempo, menos 2% do que no ano anterior consideram que a sua empresa está perfeitamente preparada para incidentes de segurança (2022: 54%; 2023: 52%). Para a pesquisa, a empresa de software OTRS Group colaborou com a empresa de pesquisa de mercado Pollfish para entrevistar 500 profissionais de TI e segurança cibernética, incluindo 100 no Brasil.

O número crescente de incidentes de segurança exige resposta rápida

Para 30%, as ameaças em rápida evolução também representam o maior desafio na resposta a incidentes. Isto é agravado pelas lacunas de comunicação entre as ferramentas (18%). Quase o mesmo número (17%), tem dificuldades com a comunicação oportuna e apropriada com o público; também 17% têm dificuldades na coordenação das equipes de resposta; e 15% com a falta de pessoal qualificado.

À luz do número crescente de incidentes de segurança, 44% consideram a sua rápida identificação o componente mais importante de um plano eficaz de resposta a incidentes. Para 21%, uma comunicação clara é a parte mais vital; para 16% é a análise da causa raiz. Por outro lado, a estratégia de remediação é de importância secundária para muitos. Apenas 13% consideram este o elemento mais crucial.

4 em cada 10 fazem pouco ou nenhum uso da automação na resposta a incidentes

A automação pode ajudar as equipes de segurança a responder mais rapidamente aos incidentes e reduzir a carga sobre sua equipe. Comparados internacionalmente, os processos de resposta a incidentes das equipas de segurança brasileiras apresentam um nível razoável de automatização. Aqui, 7% dependem inteiramente da intervenção humana para responder a incidentes. A média para todos os mercados pesquisados é de 9%. Outros 17% utilizam apenas automação básica para alertas, mas dependem fortemente da tomada de decisões humanas.

Pouco mais da metade avançou ainda mais: 58% usam regularmente a automação para tarefas rotineiras, mantendo o controle humano sobre decisões críticas. Apenas 18% automatizam o máximo possível e reduzem ao mínimo a intervenção humana.

"Ataques cibernéticos podem interromper as operações normais de uma empresa, causando perda de produtividade e receita. Ter medidas eficazes de cibersegurança ajuda a garantir a continuidade operacional, minimizando o impacto de possíveis interrupções. Além disso, as consequências de uma violação de segurança podem ser financeiramente devastadoras. Isso inclui custos de recuperação, notificação de clientes afetados, possíveis ações judiciais e a perda de negócios", destaca **Luciano Alves de Oliveira, Diretor Geral Brasil e Portugal do OTRS Group**.

A velocidade é essencial na resposta a incidentes

O fato de a velocidade ser essencial na resposta a incidentes também se reflete nas métricas que as equipas de segurança acreditam que melhor refletem a eficácia dos esforços globais de segurança cibernética da sua organização. Com 58%, o tempo médio de detecção (MTTD) é a métrica mais significativa para a maioria. A redução percentual de vulnerabilidades vem em segundo lugar com 45%. Logo atrás, com 44% vem a satisfação do usuário com medidas de segurança e para 38% a melhor métrica é o tempo médio para responder (MTTR).

Jens Bothe, Vice-Presidente de Segurança da Informação do OTRS Group, apela: “Quando se trata de defesa e resposta a incidentes de segurança, cada segundo conta para evitar grandes danos. As equipes de segurança devem ter todos os recursos necessários para se prepararem adequadamente para um incidente crítico. No entanto, muitas empresas não percebem esta necessidade até que tal incidente já tenha ocorrido. Elas precisam urgentemente preencher as lacunas de pessoal e investir em ferramentas que permitam que seus departamentos de segurança otimizem e, sempre que possível e apropriado, automatizem seus processos de resposta a incidentes”.

Sobre a Pesquisa “OTRS Spotlight: Corporate Security 2023”

Os dados utilizados são baseados em pesquisa online conduzida pela Pollfish Inc. em nome do OTRS Group, na qual participaram 500 profissionais de TI e segurança cibernética nos EUA, Alemanha, Brasil, México, Singapura e Malásia entre 5 e 8 de setembro de 2023.

Para mais resultados da segunda parte da pesquisa, consulte o infográfico disponível para download [aqui](#).

Os resultados da primeira parte da pesquisa estão disponíveis [aqui](#).



Luciano Alves de Oliveira, Diretor Geral Brasil e Portugal do OTRS Group



Fonte: OTRS, em 12.12.2023.