

Pesquisa Forcepoint™ e Instituto Ponemon revela o desafio das organizações no monitoramento de usuários privilegiados e a prevenção de ameaças internas

Pesquisa revela que a maioria dos gerentes de operações de TI e de segurança acredita que o acesso de usuários privilegiados frequentemente excede suas necessidades

13/09/2016 15:07:40

A Forcepoint™, líder global em cibersegurança, divulgou os resultados do estudo “Insegurança de Usuários Privilegiados”, realizado em parceria com o Instituto Ponemon, uma das principais organizações de pesquisas de segurança em TI, com a comparação de uma série de dados coletados entre 2011 a 2014 aos dados atuais. Embora ataques e vazamentos de informações privilegiadas continuem se multiplicando, o estudo descobriu que 58% dos gerentes de TI e de Segurança da Informação acreditam que suas organizações estão concedendo acesso desnecessário a funcionários que vai além de suas funções ou responsabilidades, e com 91% prevendo um número igual ou maior de ameaças internas.

Mais de 40% dos entrevistados concordam que insiders maliciosos usariam a engenharia social para obter acesso privilegiado - um aumento de 20% comparado a 2011, e não é surpresa que a maioria dos entrevistados prevê que as ameaças internas devam continuar representando um problema. Mais de 600 gerentes de operações de TI de empresas comerciais e 142 de federais, incluindo gestores de segurança, participaram do estudo.

Aproximadamente 70% de ambos os grupos pesquisados acham que é “muito provável” ou “provável” que os usuários privilegiados acreditam que têm o direito de acessar todas as informações que podem visualizar. Quase 70% dos pesquisados também acreditam que usuários privilegiados acessam dados confidenciais apenas por uma questão de curiosidade. Com esses dados percentuais em pauta, apenas 43% das organizações comerciais e 51% de organizações federais disseram que atualmente possuem a capacidade efetiva de controlar as atividades de usuários privilegiados. A maioria revelou que apenas 10% ou menos do seu orçamento é dedicado a combater esse desafio.

Enquanto o orçamento e o elemento humano são fatores importantes na hora de enfrentar o desafio das ameaças internas, deficiências tecnológicas também desempenham um papel importante. A pesquisa constatou que um número significativo dos entrevistados utiliza suas atuais ferramentas de cibersegurança para combater ameaças internas, ao invés de tecnologias mais específicas – por exemplo, 48% das organizações comerciais e 52% das federais usam SIEM (Security Information

and Event Management) para determinar se uma ação representa uma ameaça interna. Além disso, mais de 60% apontam que estas ferramentas apresentam muitos falsos positivos. Como resultado, a maioria desses públicos (63% das organizações comerciais e 75% das organizações federais) não possui a informação contextual necessária para evitar ameaças internas.

“A melhor abordagem para mitigar o abuso realizado por usuários privilegiados é uma abordagem abrangente e em camadas que implementa as melhores práticas, incorpora processos e tecnologias e, mais importante ainda, aborda as pessoas por trás das permissões”, disse Michael Crouse, Diretor Técnico de Soluções para Ameaças Internas da Forcepoint. “Os danos causados por usuários privilegiados é o mais extenso, mais difícil de mitigar e mais difícil de detectar, pois são causados por usuários autorizados a realizar ações que têm permissão de fazer. Este relatório destaca a enorme disparidade entre o fato das organizações estarem conscientes do problema e sua capacidade de resolvê-lo”.

Para o relatório completo, acesse: <https://www.forcepoint.com/privileged-user>

Infográficos adicionais podem ser encontrados aqui:

<https://www.forcepoint.com/resources/infographics/privileged-user-case-study-infographic>

<https://www.forcepoint.com/resources/infographics/privileged-user-case-study-infographic-federal>