Empresas & Negócios

Matéria de capa

Ongkantong_CANVA

DESAFIOS SE INTENSIFICARAM

A SEGURANÇA DA INFORMAÇÃO NAS INSTITUIÇÕES FINANCEIRAS: UM DESAFIO EM CONSTANTE EVOLUÇÃO

Os departamentos de cibersegurança das instituições financeiras sempre enfrentaram grandes desafios e, hoje em dia, esses desafios se intensificaram devido à crescente sofisticação dos cibercriminosos, que combinam diversas técnicas para gerar ameaças maiores e mais frequentes. Essa pressão constante testa a capacidade das equipes de segurança de proteger a reputação e os rendimentos de suas organizações.

"As instituições que dependem do mundo digital para realizar suas operações, como a área financeira, estão entre as mais visadas quando o assunto é cibersegurança. Qualquer deslize pode abrir portas para um ataque capaz de afetar não só a parte financeira, mas sua imagem frente a clientes, parceiros e fornecedores - que pode ser irreparável ou levar anos para se recuperar", afirma Helder Ferrão, gerente de estratégia de indústrias da Akamai LATAM.

Segmentação – Uma estratégia-chave para mitigar os riscos - Uma estratégia amplamente recomendada para mitigar esses riscos é a segmentação da rede. Segundo o relatório "O estado da Segmentação 2023, superando os obstáculos de implantação transformacional", realizado pela Akamai, empresa na nuvem que potencia e protege a vida online, as instituições de serviços financeiros de várias regiões (EUA, LATAM, EMEA e APAC) reconhecem a eficácia da segmentação para proteger seus recursos.

No entanto, a implementação dessa estratégia em torno de aplicativos e recursos empresariais críticos tem sido mais lenta do que o esperado. A segmentação consiste em dividir uma rede em partes menores para melhorar o desempenho e a segurança. A micro segmentação leva esse conceito um passo adiante, dividindo a rede até o nível de carga de trabalho individual e aplicando controles de segurança específicos a cada segmento.

Embora a segmentação em geral tenha progredido lentamente, as instituições que persistiram em sua implantação conseguiram reduzir significativamente seus riscos.

O aumento dos ataques ransomware e a resposta do setor – O aumento dos ataques de ransomware é um sinal claro da vulnerabilidade persistente no setor financeiro.

Funtap_CANVA

Nos últimos dois anos, o número de ataques desse tipo a instituições financeiras aumentou quase 50%, passando de uma média de 43 em 2021 para 62 em 2023. A região da Ásia-Pacífico (APAC) foi a mais afetada, com uma média de 73 ataques, enquanto a LATAM registrou 48 ataques nos últimos 12 meses.

Lembrando que aqui estamos usando apenas os números oficiais onde os casos foram relatados pelas instituições. Na verdade, sabe-se que a quantidade de casos é maior, pois nem sempre as instituições se veem obrigadas a reportar.

wing_wing_CANVA

Apesar da aparente robustez das medidas de segurança do setor, esses números destacam a necessidade de uma resposta proativa e contínua.

Não é surpreendente que as instituições da LATAM sejam as mais ativas na aplicação de estratégias de segmentação, as quais representam um alto percentual de segurança e apresentam uma média menor de ataques de ransomware em comparação com outras regiões.

Avanços em cibersegurança e Zero Trust – O risco crescente nas instituições financeiras fez com que o foco na segurança se tornasse uma prioridade, aumentando a atualização contínua de 3% em 2021 para 18% em 2023. Essa mudança responde tanto às ameaças de ransomware quanto a uma variedade de ataques em constante mudança.

66% dos entrevistados no setor financeiro consideram extremamente importante a segmentação para enfrentar o malware, e 92% a veem como fundamental para prevenir ataques. A segmentação também é chave para o modelo de Confiança Zero (Zero Trust), com 99% das organizações avançando nesse quadro, embora apenas 47% tenham completado a implementação.

A maioria das instituições financeiras deseja implantar a micro segmentação: 88% a consideram de alta prioridade, especialmente na América Latina, com 50%. 99% dos responsáveis de TI do setor consideram que a micro segmentação já é uma realidade.

Desafios no desenvolvimento da segmentação – A segmentação enfrentou vários obstáculos, como obstáculos de desempenho (41%), falta de competências e experiência (39%) e requisitos normativos (35%). A escassez de talentos em cibersegurança e a rápida evolução das ameaças contribuem para essas dificuldades.

No entanto, proteger e segmentar mais ativos resulta em uma melhoria imediata da segurança, permitindo que as equipes de segurança identifiquem e respondam aos ataques com maior eficácia.

Uma segmentação bem implementada não só melhora a proteção cibernética, mas também facilita uma recuperação mais rápida após uma infiltração, com uma redução de 13 horas no tempo de recuperação e uma redução de 11 horas na detecção de um deslocamento do ataque para apenas 3 horas.

As instituições financeiras que priorizam e aplicam persistentemente estratégias de segmentação estão em melhor posição para se defender contra as ciberameaças. À medida que mais organizações adotam e aperfeiçoam suas arquiteturas de Zero Trust, o setor financeiro pode esperar uma maior segurança e resiliência frente a futuros vetores de ameaça. - Fonte e mais informações: (https://www.akamai.com).