POR RUI DAMIÃO

EXTERNAL ATTACK SURFACE MANAGEMENT: DE OPÇÃO ESTRATÉGICA A NECESSIDADE OPERACIONAL

A EXPANSÃO DA SUPERFÍCIE DE ATAQUE EXTERNA CRIOU UM PONTO CEGO PARA AS ORGANIZAÇÕES MODERNAS: A IMPOSSIBILIDADE DE PROTEGER ATIVOS DIGITAIS DESCONHECIDOS. O EXTERNAL ATTACK SURFACE MANAGEMENT EMERGIU COMO UMA DISCIPLINA FUNDAMENTAL QUE PERMITE DESCOBRIR, MONITORIZAR E PROTEGER CONTINUAMENTE OS ATIVOS EXPOSTOS NA INTERNET

A superfície de ataque externa das organizações tem vindo a expandir-se na última década. A transformação digital acelerada, a adoção mássica de serviços cloud e a proliferação de dispositivos IoT contribuíram para esse crescimento.

O que antes se limitava a alguns servidores web e sistemas de email corporativo, evoluiu, agora, para um ecossistema complexo de aplicações SaaS, API, infraestrutura multicloud e um sem número de ativos digitais que, por vezes, são desconhecidos para os próprios departamentos de IT.

Esta evolução representa um desafio crítico para os líderes de cibersegurança. O External Attack Surface Management (EASM) emerge como uma disciplina essencial para restaurar uma visibilidade que pode ter sido perdida. Mais do que uma ferramenta tecnológica é uma abordagem estratégica que permite às organizações descobrir, inventariar, monitorizar e proteger continuamente todos os ativos digitais expostos externamente.

GERIR A SUPERFÍCIE DE ATAQUE

Ricardo Oliveira, CISO da Eurotux, explica que "a grande diferença" entre o External Attack Surface Management das práticas tradicionais de gestão de vulnerabilidades está "na perspetiva e na abordagem". "Enquanto a gestão tradicional de vulnerabilidades parte do princípio de que conhecemos todo o nosso ambiente — os ativos, sistemas, aplicações — o EASM parte de uma visão externa, como se fosse um atacante a tentar descobrir os pontos de entrada. O foco está na identificação contínua de ativos expostos, muitas vezes desconhecidos ou esquecidos, como domínios antigos, aplicações em *shadow IT* ou API públicas", explica.

Enrique Serrano, Enterprise Account Executive da Qualys Ibéria, explica que, "à medida que a superfície de ataque continua a evoluir, as equipas de cibersegurança têm vindo a recorrer a múltiplas soluções e fontes dispersas" que "proporcionam uma descoberta limitada e originam lacunas de visibilidade, dados de risco não estruturados e um grande esforço manual". Por outro lado, o EASM, foi "concebido para identificar ativos expostos e riscos a partir da perspetiva de um atacante".

Milton Silva, Cybersecurity Team Leader da VisionWare, menciona a "abordagem *outside-in*" do EASM, centrada naquilo que um atacante veria e poderia explorar, explicando que "visa identificar e monitorizar continuamente todos os ativos expostos à Internet, incluindo domínios, subdomínios, serviços em cloud e infraestruturas esquecidas". Assim, diz, "a gestão tradicional parte de um inventário de ativos conhecido, muitas vezes limitado à infraestrutura interna

e ao que está sob controlo direto da organização, enquanto o EASM atua de forma contínua e automatizada para identificar todos os ativos expostos".

Já André Alves, NOC/SOC Team Leader da Warpcom, explica que o External Attack Surface Management se distingue das práticas tradicionais de gestão de vulnerabilidades pelo "seu foco na descoberta contínua e automatizada de ativos expostos na Internet e muitas vezes fora do inventário oficial". Assim, diz, "enquanto as soluções de *vulnerability management* se focam mais em ativos conhecidos como servidores internos, aplicações catalogadas, redes corporativas e funcionam com scans periódicos, as ferramentas de EASM mapeiam de forma proativa subdomínios abandonados, API públicas e recursos em cloud que podem escapar à perceção manual".

OS DESAFIOS DE IMPLEMENTAÇÃO

Enrique Serrano menciona que os ativos desconhecidos continuam "a representar uma fatia importante do risco nas organizações" e que "gerir

O "PRIMEIRO" DESAFIO É "A DESCOBERTA INICIAL DE ATIVOS", SEGUIDO DA "INTEGRAÇÃO DO EASM COM PROCESSOS INTERNOS". POR FIM, OUTRO DESAFIO É A COORDENAÇÃO ENTRE EQUIPAS: SEGURANÇA, OPERAÇÕES, DESENVOLVIMENTO, IT... É PRECISO ORQUESTRAR VÁRIAS ÁREAS PARA QUE O PROGRAMA TENHA IMPACTO".


RICARDO OLIVEIRA, CISO DA EUROTUX

esses ativos exige métodos eficazes de gestão da superfície de ataque". No entanto, diz, "é necessário um esforço significativo de planeamento e integração. O crescimento da computação na nuvem e o teletrabalho, que tornam difícil delimitar fronteiras entre o que é público e o que é privado, também vieram complicar esta gestão".

Para Milton Silva, a implementação eficaz de um programa de EASM "não é isenta de dificuldades". Um dos principais desafios apontados pelo representante da VisionWare é a "ausência de visibilidade

completa sobre os ativos externos e muitas organizações descobrem, com surpresa, que têm dezenas ou centenas de elementos expostos que não constam em nenhum inventário oficial". Outro problema, refere, é "a fragmentação das responsabilidades internas, já que diferentes equipas podem gerir ativos sem coordenação com as equipas de cibersegurança".

André Alves ressalva que "a implementação de um programa eficaz de EASM está longe de ser apenas uma questão tecnológica". O NOC/SOC Team Leader refere, também que "novos subdomínios, API e serviços cloud surgem a cada sprint de desenvolvimento, e sem uma integração eficaz


ENRIQUE SERRANO, QUALYS IBÉRIA

com as equipas de IT e DevOps, muitos destes ativos permanecem fora do radar. Mesmo quando a descoberta funciona, há outro obstáculo: o ruído.

"É NECESSÁRIO UM ESFORÇO SIGNIFICATIVO DE PLANEAMENTO E INTEGRAÇÃO. O CRESCIMENTO DA COMPUTAÇÃO NA NUVEM E O TELETRABALHO, QUE TORNAM DIFÍCIL DELIMITAR FRONTEIRAS ENTRE O QUE É PÚBLICO E O QUE É PRIVADO, TAMBÉM VIERAM COMPLICAR ESTA GESTÃO"

Plataformas de EASM mal afinadas podem gerar um volume elevado de falsos positivos, alertas sobre ativos desatualizados, irrelevantes ou sem ligação direta à organização".

Para Ricardo Oliveira, o "primeiro" desafio é "a descoberta inicial de ativos", seguido da "integração do EASM com processos internos". Por fim, outro desafio é "a coordenação entre equipas: segurança, operações, desenvolvimento, IT... é preciso orquestrar várias áreas para que o programa tenha impacto".

ERROS MAIS COMUNS

Milton Silva explica que um dos erros mais comuns é encarar o EASM "como uma tarefa pontual, em vez de um processo contínuo". Outro erro, afirma, é "confiar cegamente na automação sem envolvimento humano: apesar das ferramentas serem cada vez mais inteligentes, a validação e interpretação dos dados continua a ser essencial. Também vemos organizações que tratam todos os alertas como equivalentes, sem priorização adequa-

da, o que conduz à fadiga operacional e à perda de foco nos riscos críticos".

André Alves defende que, entre os erros mais comuns, se destaca a "definição de âmbito demasiado ampla, ou seja, ativar a descoberta em toda a Internet sem critérios de filtragem" que "leva a milhares de recursos sem importância". Também é frequente "esquecer o envolvimento de equipas de DevOps ou de gestão das plataformas cloud, o que cria silos de informação e dificulta a correção rápida", alerta o representante da Warpcom.

"Um erro frequente é assumir que a ferramenta, por si só, resolve o problema", afirma Ricardo Oliveira, acrescentando que "O EASM não é *plug-and-play*; requer contexto, análise e ação contínua". Outro erro apontado pelo CISO da Eurotux é "não envolver as equipas certas desde o início, o que leva a resistência ou fraca priorização das descobertas. Finalmente, há uma tendência para ignorar ativos 'não oficiais', quando são precisamente esses que representam maior risco".


MILTON SILVA, VISIONWARE

Para Enrique Serrano, o erro mais frequente é "encarar o EASM como mais uma tarefa para a equipa de segurança: mais um painel para consultar, mais um separador no navegador, mais fadiga de alertas". No entanto, explica, o EASM deve "reduzir as tarefas (e o stress) da equipa de segurança, ao automatizar e priorizar os fluxos de trabalho".

OBTER VALOR SIGNIFICATIVO

Com base na sua experiência, André Alves afirma que, em média, "são necessários entre três e seis

"OS BENEFÍCIOS DO EASM SÃO RAPIDAMENTE PERCETÍVEIS, SOBRETUDO QUANDO SÃO IDENTIFICADOS ATIVOS CRÍTICOS EXPOSTOS E DESCONHECIDOS. NO ENTANTO, PARA QUE O VALOR SEJA SUSTENTADO – COM PROCESSOS BEM INTEGRADOS, MÉTRICAS ESTABELECIDAS E CAPACIDADE DE RESPOSTA EFICAZ – É COMUM QUE O RETORNO MAIS COMPLETO OCORRA ENTRE ALGUNS MESES APÓS A IMPLEMENTAÇÃO"

meses" para obter valor significativa após a implementação da solução de EASM. No primeiro mês, costuma-se mapear 80% a 90% dos ativos externos e identificar os grandes ângulos mortos. Nos dois a três meses seguintes, os esforços centram-se na remediação das vulnerabilidades de maior gravidade. Até ao sexto mês, explica, "já será expectável ter algumas automatizações e integrações".

Na mesma linha, Ricardo Oliveira diz que, nas primeiras semanas, já se identificam riscos importantes. No entanto, "para atingir um valor sustentado, com processos afinados e integração com outras áreas de segurança, falamos em três e seis meses. A curva de maturidade depende muito do grau de visibilidade e colaboração interna".

Enrique Serrano ressalva que o tempo médio para obter valor pode "variar bastante consoante o tamanho e a complexidade do ambiente, o grau de maturidade das organizações, os recursos disponíveis e, claro, o tipo de solução de EASM a adotar". Considerando todas as fases, estima-se um período entre um e dois meses". Assumindo que há algumas soluções que "conseguem gerar visibilidade em poucas horas ou dias", uma "implementação bem integrada exige várias semanas de trabalho".

Milton Silva defende que "os benefícios do EASM são rapidamente percetíveis, sobretudo quando são identificados ativos críticos expostos e desconhecidos. No entanto, para que o valor seja sustentado – com processos bem integrados, métricas estabelecidas e capacidade de resposta eficaz – é comum que o retorno mais completo ocorra entre alguns meses após a implementação, dependendo da maturidade da organização e da sua capacidade de adaptação e resposta".

CASOS DE USO

Enrique Serrano destaca casos como subdomínios não registados ou aplicações de *shadow IT*, onde o EASM consegue identificar automaticamente novos domínios ou serviços, mesmo que não estejam registados. Outro exemplo, diz, é "o de certificados de domínio que permitem acesso a redes VPN sem autenticação".

Ricardo Oliveira, por sua vez, refere um caso em que "a ferramenta de EASM identificou um domí-


ANDRÉ ALVES, WARPCOM

"SÃO NECESSÁRIOS ENTRE TRÊS E SEIS MESES" PARA OBTER VALOR SIGNIFICATIVA APÓS A IMPLEMENTAÇÃO DA SOLUÇÃO DE EASM. NO PRIMEIRO MÊS, COSTUMA-SE MAPEAR 80% A 90% DOS ATIVOS EXTERNOS E IDENTIFICAR OS GRANDES ÂNGULOS MORTOS"

nio antigo, ainda ativo, usado numa campanha de marketing há anos, mas que redirecionava para um subdomínio comprometido. Nenhuma ferramenta interna detetava esse fluxo porque já não fazia parte do inventário oficial. Essa descoberta permitiu evitar um potencial abuso reputacional e risco de phishing".

Milton Silva dá o exemplo da Signify que enfrentava um risco de fuga de propriedade intelectual devido ao armazenamento não autorizado de documentos sensíveis. Através da utilização de uma solução de EASM da CybelAngel, foi possível detetar que um ex-funcionário tinha armazenado centenas de documentos de design confidenciais num servidor pessoal não protegido e a exposição desses documentos poderia ter comprometido a posição competitiva da empresa e das marcas parcerias.

Por fim, André Alves partilha "um caso muito concreto que exemplifica o valor de uma solução de EASM aconteceu com uma organização que havia terminado um projeto de migração para a cloud. A plataforma de EASM identificou um subdomínio ativo, associado a um ambiente de pré-produção antigo, que estava exposto publicamente na Internet. Esse subdomínio não estava inventariado por outras ferramentas de segurança interna, como o scanner de vulnerabilidades tradicional ou o SIEM, uma vez que já não fazia parte do ambiente de produção nem estava integrado nos fluxos normais de monitorização. Este tipo de exposição é muitas vezes ignorado por ferramentas internas, porque vive fora do perímetro conhecido ou controlado. A solução de EASM destacou este ativo precisamente por ter como base uma lógica externa, semelhante à de um atacante: procurar tudo o que é visível da Internet, independentemente da origem ou da visibilidade interna. Graças à descoberta atempada, foi possível desativar o serviço antes de qualquer exploração. O incidente deu origem à revisão dos processos de desativação de ambientes e reforçou a necessidade de visibilidade contínua sobre a