TANIUM

O guia definitivo para a higiene cibernética

A higiene cibernética consiste em planejar, de forma proativa, uma estratégia de segurança para evitar ataques cibernéticos.

O modo de trabalho misto dos trabalhadores tem ampliado a superfície dos ataques, e os crimes cibernéticos estão mais sofisticados. Isto é evidente ao observar rapidamente as últimas notícias que contam histórias de redes de governos, organismos públicos e empresas privadas que se tornam alvos de ransomware.

E as ameaças são cada vez mais audaciosas.

É fundamental que as organizações tenham consciência de sua posição de risco e contem com ferramentas que proporcionem a visibilidade e o controle de pontos de extremidade (também chamados de terminais ou endpoints) necessários para detectar e pôr fim às ameaças. Mas as ferramentas, por si só, são apenas a metade da equação. Os responsáveis por TI sabem que, para manter e proteger as redes empresariais, é necessário implementar as ferramentas adequadas, com as práticas de higiene recomendadas, a fim de obter melhores resultados.

A higiene da TI ou higiene cibernética é fundamental para a segurança e o gerenciamento dos sistemas das empresas. Para melhorar a higiene cibernética, é necessário criar um processo para identificar continuamente ativos, riscos e vulnerabilidades em determinado ambiente e solucioná-los rapidamente na escala correspondente. Concentrar-se na higiene cibernética pode ajudar a prevenir muitas das violações, interrupções e contratempos dos quais as empresas são vítimas.

À medida que os ambientes aumentam de tamanho e complexidade, ampliam-se a variedade de dispositivos e as cargas de trabalho. As organizações devem gerenciar tudo, desde computadores portáteis e máquinas virtuais (VM) até contêineres através de amplas redes distribuídas que englobam vários escritórios e, inclusive, continentes. Mediante essas exigências, a higiene cibernética se vê afetada com frequência.

Neste e-book, explicaremos os componentes da higiene cibernética e a forma como várias ferramentas contribuem ou frustram os esforços para melhorá-la.

Saber o que se tem

Para preservar e melhorar a higiene cibernética, é preciso saber quais são os ativos que você tem. Há 50, 100 ou 500 mil computadores e servidores em sua organização? Onde estão? Quais são? O que eles têm instalado? Quais serviços proporcionam?

A resposta a essas perguntas constitui a detecção e o inventário de ativos. É a base da higiene cibernética.

Neste capítulo, aprofundaremos nos motivos pelos quais essa base é tão importante.

Quem não sabe o que tem não pode gerenciar?

São necessários três níveis de conhecimento para gerenciar seus pontos de extremidade:

- Quais ativos você tem e onde estão
- Quais softwares estão sendo executados neles e se estão licenciados?
- Como as máquinas de sua rede se relacionam entre si e qual é o seu propósito?

Todas as empresas, independentemente do porte, precisam dessas informações, que, na TI moderna, mudam constantemente. Os ativos de rede vêm e vão, especialmente com os critérios do esquema “traga seu próprio dispositivo” (BYOD, sigla em inglês), uma política cada vez mais presente e em crescimento em muitas organizações.

Alguns ativos podem aparecer na rede só ocasionalmente. E com mais empresas que incentivam os funcionários a trabalhar em casa (WFH, sigla em inglês), a complexidade aumenta ainda mais.

As desvantagens operacionais do não saber

Parafraseando Dom Henley, um músico norte-americano e antigo membro da banda The Eagles, quando você dirige com os olhos fechados, com certeza, acabará batendo em algo.

Provavelmente, uma das primeiras coisas com a qual você se deparará é a vulnerabilidade da segurança. Se não puder gerenciar um ativo, você não conseguirá protegê-lo. E não conseguirá gerenciá-lo se não souber que ele existe. É possível que haja vetores de ataque que você desconheça totalmente, como uma vulnerabilidade não corrigida.

E quais são as implicações econômicas? Você tem uma ideia geral sobre onde está gastando o dinheiro? Tome, por exemplo, as licenças de software de um programa popular como o Microsoft 365. Se tem uma licença para 10 mil cópias, você usa 20 mil ou só 5 mil? Você utiliza eficientemente a licença que paga? Ou está descumprindo a lei e exposto a ações judiciais dispendiosas?

Além disso, a conformidade não diz respeito somente às licenças de software. Tomemos os serviços de saúde como exemplo. As instituições de saúde devem demonstrar conformidade com as disposições da HIPAA e da PCI, que abrangem informações protegidas sobre saúde e os dados de cartões de crédito. Você sabe onde residem esses dados? Se não souber, não será possível demonstrar sua conformidade. A incapacidade de demonstrar a conformidade tem dois inconvenientes importantes: sanções normativas e clientes insatisfeitos.

Quais características são importantes para um conjunto de ferramentas destinado à detecção e ao inventário de ativos?

As ferramentas ou a plataforma que você utiliza para a detecção e o inventário de ativos devem oferecer:

- Exatidão
- Velocidade
- Escala
- Facilidade de uso

A exatidão, a velocidade e a escala estão estreitamente relacionadas. Se forem necessárias duas semanas ou um mês para fazer um inventário, quando você tiver acabado, a rede já terá mudado e, sem dúvida, acabará faltando algo.

Quanto maior for a rede, mais problemas ela apresentará. Por isso, a escala é importante. A facilidade de uso entra em jogo porque uma ferramenta difícil de configurar gera erros e as pessoas não vão querer usá-la.

As ferramentas mais antigas apresentam dificuldades com o que é exigido pela TI atual.

As ferramentas de detecção de ativos criadas há 10 anos precederam muitas das coisas com as quais os modernos ambientes de TI operam. Não são capazes de controlar a velocidade das mudanças que vemos agora. No entanto, as organizações, com frequência, continuam conectadas a ferramentas com as quais se sentem confortáveis, muitas das quais não são fáceis de usar.

De fato, podem se sentir orgulhosas de dominar as ferramentas difíceis de usar. Talvez tenham até escrito scripts personalizados para que funcionassem com mais eficiência. E não só isso: desenvolveu-se todo um ecossistema de sócios que ajuda os departamentos de TI a fazerem exatamente isso.

As consequências não previstas dessa situação são políticas e processos de TI quase artesanais, não porque sejam a melhor maneira de abordar um problema, mas porque se ajustam às capacidades das ferramentas em uso. As ferramentas mais arraigadas se transformam em parte da infraestrutura de TI. Mas as melhores políticas de TI devem ser independentes das ferramentas. Uma ferramenta construída em 1993 ou 2010 não pode oferecer essa flexibilidade.

A detecção de pontos de extremidade é um objetivo em constante movimento.

Nem todos os pontos de extremidade de uma rede são computadores de mesa, portáteis ou servidores. Há impressoras, telefones, tablets e um número cada vez maior de dispositivos tipo Internet das Coisas (IoT, sigla em inglês), tanto industriais como domésticos. O gerenciamento de dispositivos móveis (MDM, sigla em inglês) é um campo em crescimento. Com um provedor MDM, como o Microsoft Intune, você pode realizar um rastreamento de todos os telefones de uma rede.

Mas por que você deveria ter que se preocupar com o fato de um dispositivo de IoT doméstico colocar em perigo a rede corporativa? Este é o motivo:

Um funcionário de um de nossos clientes trabalhava em casa. A equipe de segurança da empresa estava recebendo alertas de que alguém estava tentando entrar em seu laptop. A fonte era um frigorífico com malware que vasculhava a rede doméstica e tentava entrar no dispositivo, que estava temporariamente na rede corporativa. O mesmo poderia ocorrer com um interruptor de luz inteligente, termostato ou câmera de segurança.

Isto se aplica também às máquinas de uma fábrica, muitas das quais estão dotadas de sensores que se comunicam através de redes sem fio com aplicativos de fabricação com interface na Internet. Chama-se tecnologia operacional e faz com que cada máquina de uma fábrica seja um dispositivo de rede.

Nenhuma ferramenta de detecção de ativos é capaz de identificar todos os tipos de dispositivos. Por isso, a ferramenta ou plataforma que você utilizar deverá ser integrada e funcionar bem com aplicativos compatíveis que possam reconhecer dispositivos como telefones, tablets, impressoras, etc.

A detecção de endpoints é a base das redes de confiança zero (ZTN, sigla em inglês).

Quando tudo é um dispositivo de rede, tudo representa uma possível vulnerabilidade de segurança. Portanto, são necessários procedimentos e políticas que dividam os pontos de extremidade em três categorias: gerenciados, não gerenciados e não gerenciáveis. A detecção de endpoints é o primeiro passo crucial na tendência rumo à confiança zero, que é uma arquitetura de segurança que supõe que não se pode confiar em nenhum dispositivo ou usuário sem verificação.

Esse é o local onde começa a higiene cibernética e a segurança.

Feche portas e janelas

Os responsáveis pelas ameaças estão melhorando na hora de encontrar links fracos, explorar vulnerabilidades e configurações erradas antes que as equipes de segurança e operações de TI tomem conhecimento delas.

A conformidade normativa está também aumentando a pressão sobre as organizações, já que estas sofrem dificuldades para gerenciar as consequências econômicas e de reputação das violações.

No centro de qualquer boa estratégia de gerenciamento de riscos cibernéticos está o gerenciamento e a configuração das vulnerabilidades.

1. Priorizar

O crescimento exponencial dos endpoints empresariais torna impossível solucionar todos os problemas de imediato. Por essa razão, é importante definir prioridades. Em primeiro lugar, trata-se de determinar a importância dos ativos de TI: laptops, servidores, máquinas virtuais, contêineres ou outros tipos de endpoints. Esse trabalho pode ser dividido entre as fases de detecção e avaliação do ciclo de vida.

Utilize os resultados da avaliação para priorizar ações baseadas na relevância dos ativos e os problemas de vulnerabilidade que os afetam. Aqui, a visibilidade e a supervisão contínuas devem ser palavras-chave.

2. Concentrar-se na correção

A correção das vulnerabilidades em tempo hábil é essencial; os atacantes agem rapidamente e melhoram continuamente seus ataques para aproveitar as brechas de segurança. Ainda que muitas equipes de segurança realizem análises frequentes e sejam suficientemente conscientes dos pontos fracos das infraestruturas, solucioná-los é outro assunto. Lançar o problema sobre as pessoas não é a resposta. Até mesmo as grandes equipes de TI podem se ver momentaneamente atordoadas com o grande número de problemas e endpoints que precisam de intervenção.

A automação faz que o ciclo de vida flua naturalmente. Para as equipes preocupadas pelos patches automatizados que rompem os sistemas críticos, os processos de avaliação secundários podem ser integrados aos fluxos de trabalho automatizados. Estes comprovam se é provável que os patches sejam relativamente benignos ou se apresentam risco.

3. Execute o rastreamento do seu ritmo de correções ao longo do tempo

Compreender a velocidade e o sucesso das correções revela a efetividade de seus esforços no gerenciamento de vulnerabilidades. Na fase de verificação, não só é preciso validar se as mudanças necessárias foram realizadas, mas também avaliar as métricas de seu rendimento.

É possível ver a rapidez de identificação de problemas, a rapidez com que sua equipe os resolve, se os contratos de serviço (SLA, sigla em inglês) são cumpridos e fazer comparações com o rendimento de seus colegas. Os dados frescos e precisos contribuem para que esta etapa do ciclo de vida seja mais completa e promovem uma cultura de melhoria contínua.

4. Automatizar em qualquer lugar que seja possível

No mundo ideal, isso envolveria automatizar todo o ciclo de vida do gerenciamento de vulnerabilidades. Isto reduziria os erros manuais e o risco cibernético, aceleraria o tempo de reparo e permitiria que as pessoas trabalhassem em outras tarefas. Mas ainda há elementos que algumas organizações podem desejar ou que precisam realizar, revisar, aprovar, auditar e validar diretamente.

Entre estes estão a peça inicial de valoração de ativos, que pode ser mais uma arte do que uma ciência, e a análise de métricas na fase de verificação. Ainda assim, sempre vale a pena avaliar periodicamente se é possível automatizar ainda mais.

5. Comece pouco a pouco para superar as resistências à mudança

Uma das maiores barreiras para modernizar o gerenciamento de vulnerabilidades são as pessoas e a cultura. Pode haver membros da equipe que sejam veementemente contra soluções automatizadas depois de elas terem causado acidentalmente uma interrupção da produção no passado através de patches automatizados. Pode haver outras pessoas que temem que seus trabalhos estejam em risco se forem utilizadas máquinas para solucionar problemas nos pontos de extremidade. Algumas simplesmente se queixam de que “não é bem assim que as coisas são feitas por aqui”.

A mudança pode ser aterrorizante, mas é também essencial promover a melhoria contínua. Colha primeiro as frutas que estão nos galhos mais baixos. Essa metáfora ensina às partes interessadas resistentes o valor dos enfoques automatizados para o gerenciamento de vulnerabilidades e como poderiam ser mais produtivas.

Experimente o inofensivo para começar, como automatizar a detecção para avaliar as fases do ciclo de vida. Uma análise automática, ativada depois de detectar um novo ativo, pode reduzir um processo que, antes, durava cinco dias e, agora, somente cinco minutos.

Quanto à correção, considere implementar patches automatizados ou atualizações de softwares para problemas de gravidade média ou baixa em ambientes não produtivos para demonstrar velocidade e eficácia antes de passar para ambientes de produção.

6. Tudo começa pela política

Por mais importante que seja a tecnologia, não esqueçamos o básico, que começa por dispor de políticas, planos e SLAs adequados. Pode ser algo tão simples como: "Vamos desenvolver um ciclo de vida de gerenciamento de vulnerabilidades que definiremos e, aqui, estão os SLAs para cada período de ciclo". Uma vez que os SLAs estejam em vigor, poderá ficar claro que as ferramentas automatizadas são a melhor maneira de conseguir determinados objetivos.

7. Buscar continuamente a redução completa dos riscos

Com muita frequência, as organizações se concentram em cumprir os requisitos mínimos de conformidade sem observar o panorama geral: o gerenciamento eficaz de vulnerabilidades é bom para a empresa.

É importante assegurar-se de que a verificação de endpoints não seja realizada simplesmente para assinalar os quadros correspondentes uma ficha de conformidades, mas como parte de uma estratégia integral de gerenciamento de riscos.

Isso significa executar análises continuamente para identificar, priorizar e solucionar os problemas à medida que eles aparecem em vez de o fazer justamente antes de uma auditoria. Lembre-se de incluir todo o ambiente de TI; não só os ativos fixos, mas também o código personalizado em desenvolvimento.

CAPÍTULO 3

Mais rapidez nas respostas

Responder a um incidente de segurança cibernética, seja quando se trata de uma violação de dados, um evento de ransomware ou algum outro tipo de ataque cibernético, pode comprometer imensamente as operações rotineiras de uma organização, além de romper a confiança pública, prejudicar o valor da marca e roubar uma grande parte dos rendimentos.

Neste capítulo, apresentaremos o marco de trabalho PICERL. Ele é composto por seis passos que as organizações podem adotar para melhorar e ajustar seus planos de resposta a incidentes. O PICERL corresponde originalmente à sigla em inglês para Preparar, Identificar, Conter, Erradicar, Recuperar e Lições aprendidas.

Passo 1. Preparar

A preparação garante que as pessoas adequadas das equipes adequadas se sintam envolvidas, compreendam suas funções e saibam o que devem fazer quando ocorrer um incidente.

A fase de preparação deve gerar um plano que as equipes de resposta a incidentes (IR, sigla em inglês) possam praticar. Os planos de IR devem ser ensaiados para que se possa enfrentar qualquer ponto fraco. As simulações ajudam os membros da equipe a agir sob a pressão de um incidente real.

Perguntamos aos clientes se sua equipe de IR já participou de uma simulação e compreendeu suas funções. Perguntamos também quem notifica as relações públicas e os departamentos jurídico e financeiro.

A fase de preparação ajuda a determinar a existência das ferramentas adequadas. Em caso negativo, há recursos para obtê-las e proporcionar a correspondente formação? Uma vez criados um plano e o orçamento de IR, a alta gerência deverá analisar e aprová-lo.

Passo 2. Identificar

Mediante um incidente, a fase de identificação é aquela em que se deve começar a tentar responder a perguntas como:

- Quando começou e como ocorreu? Roubo de senha ou ativo? Correio eletrônico de phishing? Código malicioso de um disco portátil?
- Qual foi o ponto de entrada? Foi uma vulnerabilidade não corrigida?
- Quem constatou e como?
- Qual é o alcance? Está limitado a uma ou duas pessoas ou ativos ou é mais abrangente?
- É possível continuar com a atividade? Os passos que você tomar afetarão alguma de suas linhas de negócio?

Com muita frequência, as credenciais comprometidas são o ponto de entrada. A partir daí, os mal-intencionados podem aproveitar qualquer oportunidade que encontrarem.

Passo 3. Conter

A contenção consiste em executar seu plano para evitar que o comportamento não desejado se propague. Uma estratégia de contenção em curto prazo poderia ser tão simples como emitir um comando de quarentena para evitar que um ativo, aplicativo ou sistema se comunique com qualquer coisa, salvo uma ferramenta de segurança.

A contenção em longo prazo é uma solução que se implementa em toda a empresa, mas que pode não solucionar completamente a causa raiz do incidente. Esta poderia ser uma tática para ajudar a polícia ou os órgãos reguladores. É uma boa ideia ter estratégias de contenção em longo prazo conectadas aos sistemas de cópia de segurança e recuperação de dados.

Os patches e as atualizações também fazem parte da contenção. Você tem vulnerabilidades não corrigidas relacionadas a algum incidente? Em caso positivo, é hora de acelerar o programa de patches para o aplicativo ou o software do sistema operacional em questão.

Este é também um bom momento para revisar quais usuários têm acesso como administradores e a quais sistemas. Qual é a superfície de ataque em relação com o Ative Directory? Você habilitou a autenticação multifatorial? Todos estes são problemas importantes a levar em consideração para a contenção.

Passo 4. Erradicar

Agora, você está tentando eliminar a causa da violação, a raiz e os ramos, como se diz. Isto significa, por exemplo, no caso de malware que você encontrou e eliminou de forma segura, cada instância é identificada. Você consertou e melhorou a proteção dos sistemas quando correspondia. Reimaginou sistemas cuja proteção você não pode aumentar. Atualizou sua inteligência perante ameaças para assegurar que pode identificar artefatos relacionados com a violação em questão.

Enquanto o processo se desenvolve, você pode mudar o alcance de seus esforços. Depois de um ataque de ransomware, por exemplo, é possível que haja muitos sistemas que precisem ser substituídos e restaurados desde a última cópia de segurança conhecida. Se não forem detectados todos os artefatos relacionados com o ataque ou não for solucionada a vulnerabilidade explorada para entrar no sistema, o ataque poderá se repetir.

A chave da erradicação é a minuciosidade. Encontrou tudo? Seja o que for, esta é a pergunta final. Com frequência, um sócio ou terceiro com experiência especializada pode ajudar na fase de limpeza.

Passo 5. Recuperar

O estrago já foi feito; agora é hora de se concentrar em solucioná-lo. Seja bem honesto consigo mesmo. Quando você conseguirá colocar em produção os sistemas afetados? Você criou patches para eles? Melhorou e testou a proteção? Utilizou sua equipe vermelha (um grupo que desempenha o papel de inimigo) para executar um ataque simulado contra esses sistemas utilizando as mesmas técnicas que os atacantes? Com certeza, você gostaria de poder dizer: "Solucionamos as vulnerabilidades e aqui está a prova".

A recuperação também significa definir a forma como o incidente mudará o alcance de sua supervisão. Durante quanto tempo você supervisionará a atividade que causou a violação: 30 dias, três meses, seis meses? E o que buscará? As provas da equipe vermelha ajudarão, assim como os artefatos recolhidos durante a contenção.

Tempo médio para implantar soluções

O tempo médio de correção (MTTR, sigla em inglês) é o tempo dispendido no avanço pelas fases de identificação, contenção e erradicação de seu plano de IR.

Em 2018, o relatório de violação de dados da Verizon constatou um MTTR no intervalo de 14 a 30 dias para organizações de alto rendimento. Mas há uma forte tendência entre os profissionais da segurança para reduzir essa cifra à medida que os planos de IR amadurecem e as equipes melhoram em sua prática.

Passo 6. Lições aprendidas

Este passo deve começar com uma reunião posterior à ação que inclua todos os que fizeram parte da equipe de resposta a incidentes: TI, conformidade, jurídico, relações públicas, etc.

É aqui que você tem a oportunidade de revisar e documentar o que aprendeu sobre a violação.

- Qual parte de seu plano de IR funcionou ou não?
- Houve brechas que necessitavam de mais pessoas? Foi necessário entrar em contato com um terceiro ou com uma equipe interna que não estava em sua lista de recursos?
- Segundo o incidente, é necessário mudar sua forma de operar? Você utilizou as ferramentas das quais dispunha de forma efetiva? Elas foram configuradas corretamente?
- Como foi a comunicação entre as diferentes equipes? Poderia ser melhorado?
- Na violação, houve algum aspecto relativo ao funcionário, como um ataque de phishing ou uma manipulação inadequada dos dados? Isso pode ser resolvido com treinamento?
- A vulnerabilidade explorou de forma endêmica uma linha de negócios ou estava presente em toda a organização? Seria possível resolver a vulnerabilidade com uma estrutura ou processo operacional diferente?

Quanto mais flexível for o plano de IR, mais você aprenderá com uma violação quando ela ocorrer. Tudo o que você aprender deverá voltar à fase de preparação, que sempre pode ser refinada e melhorada.

Conclusão

A realidade é que o ransomware e outras ameaças cibernéticas chegaram para ficar. As redes mais cobiçadas e a infraestrutura crítica sempre serão um alvo. A intenção deste e-book era proporcionar um entendimento amplo e conceitual do que é a higiene cibernética, bem como algumas diretrizes de higiene, práticas recomendadas e conhecimentos a ter em conta que ajudarão você a preparar as equipes de TI para defender com mais eficácia os pontos de extremidade que elas gerenciam.

É no passo entre a perspectiva e a ação que higiene cibernética costuma tropeçar. A informação se perde entre as lacunas das ferramentas e as equipes fragmentadas.

A coordenação efetiva das implementações de patches e softwares em um ambiente requer que as equipes de operações e segurança de TI trabalhem junto, sejam cooperativas e prestem contas. Para isso, é necessário implementar sistemas de base e definir claramente os fluxos de trabalho compartilhados.

A avaliação da higiene cibernética oferece visibilidade do estado de seu ambiente de TI para que se possa compreender o estado de seus endpoints, identificar brechas críticas e aprender como melhorar a higiene cibernética para reduzir as possibilidades de que sua organização apareça nas próximas manchetes de imprensa. A Tanium pode ajudá-lo neste aspecto.

Trabalhe com nossos especialistas para definir uma rota processável para um melhor gerenciamento e segurança de endpoint com uma **avaliação de riscos sem custo algum.**

Obtenha mais informações sobre como a Tanium proporciona dados e análises de alta fidelidade para pontos de extremidade, com a finalidade de fornecer informações para a tomada de decisões críticas de TI, em tanium.com →