TANIUM

Análise de TI: a base da higiene cibernética

Ferramentas e práticas recomendadas para uma empresa mais saudável, segura e distribuída.

A higiene cibernética descreve um conjunto de práticas, ferramentas e comportamentos concebidos para manter todo o ambiente de TI saudável e funcionando com máximo rendimento. Uma segurança que se orgulhe de sua solidez depende da higiene cibernética.

Este e-book explica as bases da higiene cibernética no contexto dos dados e das análises. Quais são os dados necessários e como usá-los para tomar decisões de TI mais conscientes e eficientes para sua organização?

CAPÍTULO 1

A desconexão entre as ferramentas e a política

As análises e os dados recentes podem realçar a desconexão entre as ferramentas e a política. As pessoas sentem-se vinculadas e acomodadas com certas ferramentas. Por isso, é bastante comum criarem políticas sobre o que suas ferramentas podem fazer em vez de se adaptarem ao que a situação exige. As trajetórias profissionais e os ecossistemas de sócios baseiam-se em sua capacidade de usar e manter determinadas ferramentas para determinados fins.

Este é um cenário comum. Antes de colocarem a Tanium em ação, alguns de nossos clientes tinham intervalos de manutenção de 12 horas para corrigir seus dispositivos e colocá-los em operação. O intervalo de manutenção era longo porque não podiam fazê-lo mais rápido com as ferramentas de que dispunham.

Quando demonstramos que é possível fazer mais rápido, com mais eficiência e menos tempo de inatividade, a direção da empresa vê o valor empresarial que a solução representa. Os engenheiros costumam querer seguir com as ferramentas que têm utilizado até o momento. Com frequência, é necessário um impulsor, respaldado por dados, para forçar qualquer mudança.

Operações e segurança. Colaboradores ou concorrentes?

Em um mundo perfeito, o trabalho que desempenham as equipes de Operações de TI e de Segurança se fundiria em um esforço conjunto e sem fissuras. Mas, na maioria das organizações, há uma linha divisória bem demarcada entre ambas as áreas.

Na Tanium, com frequência, você escutará a equipe de Operações dizer à de Segurança: "Nosso trabalho é a higiene e, fazendo-o bem, facilitamos a sua vida". E é verdade. Assim, os analistas forenses e os caçadores de ameaças podem se concentrar em ameaças maiores, como os hackers de alcance nacional, em lugar dos malwares tradicionais detectados por antivírus (AV) ou alertas baseados em um patch conhecido.

A tensão entre Operações e Segurança provém das diferentes perspectivas com que elas veem o mundo. A Segurança tende a querer bloquear tudo. As Operações querem que o ambiente seja seguro, mas o suficientemente aberto, para que a organização possa maximizar o rendimento na cada oportunidade apresentada. Os patches e as vulnerabilidades costumam ser onde surgem os conflitos, pois elas vivem em um limbo entre Operações e Segurança.

Quanto às Operações, existem ferramentas para tratar desses pontos antes que a Segurança possa vê-las. Se você desempenha seu trabalho em Operações, quando a equipe de Segurança diz: "Estas são as vulnerabilidades que encontramos", elas deveriam ser um número muito pequeno, porque você não está esperando que digam o que precisa ser corrigido.

E, com certeza, a experiência do usuário está neste ponto. Foram consumidos tantos recursos do sistema com ferramentas de segurança que os usuários não conseguem fazer nada? A memória se esgotou? Os aplicativos estão sendo bloqueados? É necessário ter uma forma de medir a experiência do usuário. Não há padrões neste setor que mensurem a experiência do usuário. Por isso, é preciso estabelecer os seus próprios.

A análise deve ser o idioma comum das equipes de Operações e de Segurança

A análise de TI é um tema extremamente amplo, já que as os times se estendem por vários âmbitos, como a informática, a experiência do usuário, as infraestruturas, o armazenamento e as redes. Ela apresenta diferentes significados dependendo de em que é aplicada e a quem se destinam os resultados.

Por exemplo, se pensamos na experiência do usuário final, as análises de TI podem fornecer o tempo de inicialização de um dispositivo, o tempo de início ou resposta do aplicativo, bem como os bloqueios do aplicativo durante um período, em um conjunto de dispositivos ou um departamento.

Com as pessoas desempenhando o trabalho remotamente e utilizando possivelmente escritórios virtuais, é possível observar as tendências de uso do armazenamento com o tempo e a forma como o trabalho remoto tem influenciado ou poderia influenciar a despesa com infraestruturas durante os próximos 6, 12 ou 18 meses.

As análises são orientadas para facilitar a detecção de dados relevantes, na tentativa de que os pontos de extremidade forneçam o tipo correto de relatórios, quando solicitados, e descrevendo com precisão a capacidade da rede.

As análises fornecem os dados brutos necessários para medir o rendimento da rede. A equipe de Operações utiliza esses dados para maximizar a produtividade empresarial. A equipe de Segurança os utiliza para proteger melhor a organização contra as ameaças. As análises são igualmente importantes para os departamentos de Operações e Segurança. Um enfoque de plataforma para as ferramentas, em lugar de uma solução pontual, pode criar pontes entre Operações e Segurança.

CAPÍTULO 3

O que constitui uma boa higiene cibernética?

Em saber o que se tem e realizar o controle adequado. Você possui as licenças de software necessárias? Não está em conformidade com as normas e corre risco de sanções? Está pagando por licenças que não está utilizando? Seus pontos de extremidade estão configurados corretamente?

Para avaliar a higiene cibernética, faça as seguintes perguntas para si mesmo:

- De quais dispositivos de ponto de extremidade sua empresa dispõe?
- Esses dispositivos de endpoint estão sendo gerenciados?
- Os pontos de extremidade gerenciados cumprem os critérios estabelecidos para endpoints em bom estado?

Pense em endpoints classificados em três categorias: gerenciados, não gerenciados e não gerenciáveis. Nem todos eles são computadores ou servidores. Por essa razão, uma boa higiene cibernética requer ferramentas que identifiquem e gerenciem itens como telefones celulares, impressoras e máquinas de uma fábrica. Não há uma única ferramenta que possa identificar e gerenciar todo tipo de endpoint. Mas, quanto mais visibilidade você tiver, melhor será sua higiene cibernética e sua posição de risco.

O trabalho remoto (WFH, sigla em inglês) tem tornado a visibilidade bem mais difícil. Se os pontos de extremidade nem sempre estão na rede, como medi-los? Muitas ferramentas não foram criadas para gerenciar esse cenário. Mas, uma vez que você saiba que dispositivos tem, onde estão e o que há neles, poderá aplicar políticas que garantam que os dispositivos se comportem como deveriam.

Uma boa higiene cibernética requer também corrigir e atualizar o software rapidamente. Quando a Microsoft lança os Patch Tuesdays, você consegue obter parches críticos em todos os seus dispositivos em um período razoável? Consegue saber, em tempo real, o que foi e o que não foi corrigido?

Dessa maneira, quando a equipe Segurança contata a de Operações e diz: “Há uma falha de dia zero no Microsoft Word, quantos de seus pontos de extremidade têm esta versão?”, A equipe de Operações pode responder: “Já estamos sabendo e já consertamos”. Esse é o papel da visibilidade na higiene cibernética.

Ou se o diretor financeiro (CFO) diz: “Estamos queimando dinheiro com o Adobe Acrobat. Estamos realmente utilizando todas as nossas licenças?”. Estes tipos de pergunta podem ser respondidos com uma prática coerente de higiene cibernética.

A atualização dos dados é a chave para uma análise efetiva

A importância da atualização dos dados, ou de sua definição, não é uniforme em todas as operações de TI. Por exemplo, se o hardware tem um ciclo de atualização baixo, como a cada dois ou três anos, não é significativo se a unidade de processamento central (CPU) ou os dados do modelo do disco rígido têm um mês de existência.

Mas, se você está tomando decisões sobre a retirada de servidores ou a migração de cargas de trabalho de um ambiente físico para um virtual, os dados que já têm dias de existência, muito provavelmente, causarão problemas. Você poderia retirar um servidor de uma unidade de negócio que depende de cargas de trabalho móveis e que respaldam um serviço crítico.

Este é um exemplo. A Tanium teve um cliente envolvido na certificação do Programa Federal de Gerenciamento de Riscos e Autorizações (FedRAMP). Para manter a certificação, realizavam uma auditoria para o governo federal uma vez ao ano.

A cada seis meses, pagavam um auditor externo para ver a que ponto estavam de serem aprovados ou não na auditoria. Ser aprovado na auditoria era crucial. A reprovação na auditoria colocava em risco dezenas de milhões de dólares de faturamento.

Então, implementaram a Tanium para verificar a cada quatro horas o estado dos elementos que fariam parte da auditoria. Esta mudança, ou seja, deixar de obter informações a cada seis meses e passar a recebê-las a cada quatro horas, significava que as equipes de Engenharia, Operações e DevOps, que realizavam mudanças no sistema constantemente, poderiam ver o impacto das mudanças na preparação do sistema para a auditoria. Com dados novos, o cliente sabia, todos os dias, como funcionavam seus sistemas em relação à aprovação ou à reprovação na auditoria.

Os dados antigos mentem

Os dados antigos quase nunca são precisos. Por isso, é muito provável que as decisões baseadas neles sejam errôneas. Independentemente do conjunto de dados, sejam eles de patches, conformidade, configuração de dispositivos, vulnerabilidades ou ameaças, dados antigos não são confiáveis.

A velocidade das mudanças no âmbito da TI faz com que dados atualizados sejam de vital importância. Se os dados têm até mesmo uma semana e muito menos meses de existência, seria melhor fazê-lo ao acaso do que tomar decisões baseadas em dados com 90 dias de existência, já que eles não indicam o estado atual de seus aplicativos, cargas de trabalho, clientes ou possíveis riscos de ataques cibernéticos.

Um de nossos clientes hospitalares não atualizava seu banco de dados de gerenciamento de configuração (CMDB, sigla em inglês) havia 90 dias. É como fazer um avião voar com dados de instrumentos já com 90 dias de existência. Isso é realmente subestimar o problema.

Os pilotos não precisam se preocupar com a presença de uma nova montanha ou um novo arranha-céus a cada duas semanas. Mas, em TI, o equivalente a uma nova montanha pode surgir em questão de horas ou dias.

O hospital estava decidindo quais cargas de trabalho interromper, virtualizar ou transferir para a nuvem, partindo de dados com 90 dias de existência. A Tanium forneceu dados precisos e em tempo hábil. Deixaram de usar dados obsoletos e passaram a usar dados que tinham um dia de existência. Desde adivinhar até tomar decisões conscientes.

Um bom lugar para começar. Seis práticas recomendadas de higiene cibernética.

Para ter uma visão geral do que podem fazer os dados, as análises e a higiene cibernética, estas são seis práticas recomendadas que abrangem seus fundamentos:

- Crie um inventário preciso de tudo o que está conectado à sua rede, tanto gerenciado como não gerenciado.
- Documente o que há nos dispositivos: software, dados e processos.
- Avalie as vulnerabilidades e o estado dos patches para determinar as posições de risco.
- Assegure-se de que softwares de terceiros, como Adobe, Microsoft Office, Google Chrome, etc., recebem a mesma atenção que os softwares de sistema operacional (SO).
- Não descuide do gerenciamento da configuração. Conheça onde se aplicam as políticas do grupo e esteja seguro de que todos os dispositivos cumpram os requisitos mínimos.
- Feche os controles de acesso a serviços e dispositivos. Elimine os direitos de administrador local fornecendo aos empregados capacidades de autosserviço limitadas para instalar softwares por meio de uma interface controlada.

Ao colocar em prática estas seis coisas, você terá uma ideia mais precisa de onde concentrar esforços para dotar a organização de uma melhor higiene cibernética. Por exemplo, se os dispositivos de sua estação de trabalho têm uma pior posição de risco do que a de seus servidores, saiba que é preciso observar os dispositivos informáticos do usuário final. Isto costuma significar assegurar-se de que o SO e os patches de softwares de terceiros sejam aplicados diligentemente.

CAPÍTULO 5

Análise de TI e capacidade de dados de rede

Seja uma oficina com 5 ou 100 mil pontos de extremidade, a transmissão de grandes quantidades de dados em tempo real requer uma largura de banda de rede para transportá-los. É possível que você não disponha da infraestrutura necessária para gerenciar dados em tempo real de todos os sistemas que esteja operando. Assim, concentre-se no básico.

Isto significa que, como organização, você precisa compreender e identificar os principais serviços e aplicativos que mais necessitam de dados novos. Esses são os serviços que mantêm um negócio em funcionamento. Com esses dados, você poderá filtrar o ruído e ver como estão suas operações de TI e as posições de segurança desses sistemas.

Para simplificar a recompilação dos dados corretos, agilize os fluxos de trabalho

Uma vez identificados os serviços principais, como são os fluxos de trabalho com suas ferramentas? A maioria das organizações tem uma mentalidade do tipo “minhas ferramentas ditam meu fluxo de trabalho”. Esta é uma visão antiquada.

Articule o objetivo. Você deseja uma rede de alto rendimento, baixa vulnerabilidade e uma potente resposta contra ameaças. Portanto, quer ferramentas que possam servir seus sistemas centrais, fazer patches eficientes, executar proteção antivírus e gerenciar a recuperação em caso de alguma violação. Isso é o que suas ferramentas deveriam suportar.

Seus fluxos de trabalho deveriam ajudar a eliminar as ferramentas que não são adequadas para seu negócio.

Análise e experiência do usuário

Quando algo deixa de funcionar, é preciso dispor de uma forma de medir o impacto. Suponhamos que você tenha encerrado 10 vulnerabilidades de pontos de extremidade. Seus aplicativos estão falhando ou utilizando mais recursos? Você tem mais sistemas com 100% de uso de CPU do que antes? Isso significa que ninguém pode utilizar esses sistemas. É aqui que a análise se faz necessária. Caso contrário, você só está fazendo adivinhações. Você não pode depender dos usuários para obter informações confiáveis e em tempo hábil.

Para eliminar parte da carga do serviço de assistência, muitas grandes organizações concedem a todos os usuários direitos de administração. Mas isso pode afetar as ferramentas de segurança nos pontos de extremidade. É um atalho que as organizações utilizam para ter menos chamadas ao serviço de assistência e reduzir a frustração do usuário porque não conseguem identificar antecipadamente aqueles sistemas que, provavelmente, vão apresentar problemas. Não têm outra coisa a medir se não o consumo de recursos, algo que é realizado periodicamente nos servidores, mas não em dispositivos de usuário. Por isso, não têm nenhuma ideia da experiência do usuário.

As métricas de rendimento são fundamentais. Por exemplo, quando a equipe de Segurança deseja instalar mais cinco agentes, a equipe de Operações pode mostrar sistemas de usuário que já estão funcionando com 75% de sua capacidade máxima. A adição dessas ferramentas pode significar que os usuários não consigam trabalhar. Estas são as análises que respaldam as decisões empresariais.

É importante encontrar ferramentas que respaldem suas políticas. Mas, uma parte desse suporte que, com frequência, passa despercebida é a capacidade da ferramenta na hora de fornecer informações em tempo real para os engenheiros e em um formato que indique se os objetivos da política estão sendo cumpridos.

Análise para alta gerência

A principal preocupação da alta gerência é: “Será que meus usuários conseguem realizar seu trabalho?” Muitas decisões de TI se baseiam no risco: o risco de que os sistemas de TI se interponham no caminho que os empregados usam para trabalhar. Mas tomar essas decisões sem dados que as avaliem costuma implicar em problemas.

Você não pode tomar decisões baseadas no que dizem alguns usuários e projetá-las para toda a organização. Assim, é preciso perguntar: “Será que meus usuários conseguem fazer o trabalho para o qual foram contratados e meus dispositivos são seguros?” Onde está essa linha em sua organização? Por essa razão, a alta gerência necessita de análises.

Algumas organizações só aplicam patches nos sistemas operacionais porque acham que existe um risco excessivo de sofrerem tempos de inatividade se forem aplicados em aplicativos de produtividade, como o Microsoft Office. Não têm como testá-los e, por isso, não os corrigem. Além disso, acham que seus sistemas não podem ser atacados por um desses aplicativos, o que não é verdade. Não estão traçando a linha entre segurança e usabilidade a partir de dados.

Os executivos precisam de análises resumidas

É aí que os painéis de nível executivo que mostram indicadores-chave e de fácil gerenciamento sobre o estado da TI podem ajudar a averiguar, com dados, onde traçar a linha entre a segurança e o risco operacional.

Por exemplo, se um indicador-chave mostra que faltam patches críticos para 20% dos sistemas da organização, este é motivo de preocupação. No entanto, se o painel mostra que, no mês passado, a cifra era de 50%, a tendência segue na direção correta. Os painéis devem mostrar o estado atual e a tendência histórica.

Se há um problema em nível de resumo, os executivos podem alertar suas equipes de TI para que se aprofundem. Não precisam conhecer os detalhes; só precisam saber que os limiares ou padrões aprovados não estão sendo cumpridos.

Estes são três indicadores-chave que um painel executivo poderia incluir:

- Porcentagem de sistemas com ferramentas de segurança básicas.
- Porcentagem de sistemas vulneráveis por falta de patches.
- Porcentagem de sistemas que funcionam acima ou abaixo de um limiar de rendimento predefinido: CPU, RAM, utilização de disco, etc.

Análise operacional destinada à alta gerência

Para diretores de informação (CIO) e diretores financeiros (CFO), o papel que desempenham as análises pode ser algo mais limitado. Os CIOs precisam de análises que indiquem quais problemas de TI afetam um serviço da empresa ou um aplicativo que gera renda ao longo do tempo. Quantas falhas de aplicativos e alertas de CPU e memória estão afetando os componentes de TI que oferecem o serviço? E como é afetada a experiência do usuário?

Outra métrica importante para os CIOs está relacionada com a causa e o efeito. 30% dos usuários têm problemas de rendimento ou falhas nos aplicativos depois de realizarem mudanças durante um intervalo de manutenção? Este nível de análise é extremamente importante do ponto de vista dos serviços empresariais, bem como para a experiência dos empregados.

Os CFOs podem ter um problema financeiro ou jurídico quanto à conformidade das licenças. Por quantas licenças do Windows 10 estão pagando? Ou, o serviço de faturamento do cliente funciona corretamente?

O diretor de marketing (CMO) de uma empresa de comércio eletrônico precisa saber se o site do cliente funciona corretamente. Talvez esteja sobrecarregado com os pedidos da Black Friday.

O diretor de segurança da informação (CISO) quer conhecer os níveis de patches. A resolução deste heterogêneo grupo de problemas de rendimento depende de dados atualizados para obter precisão.

Se as organizações dispõem de ferramentas que podem acessar esses dados rapidamente, o próximo passo é criar uma capa de visualização de dados que não sobrecarregue os executivos com excesso de detalhes.

Análise para engenheiros

Quando surge um problema é fundamental que os engenheiros tenham acesso a dados em tempo real ou quase real em todos os seus sistemas a partir de um só lugar. Sem esse acesso, eles se veriam obrigados a comprovar os sistemas de forma pontual ou esperar até que recebessem o próximo relatório programado. Por fim, ficam sem saber quais informações são ou não são precisas. A equipe de engenharia deve sempre conhecer os problemas antes que a equipe de direção o faça. Preferencialmente, o problema deve ser resolvido antes que chegue ao painel de controle executivo.

A análise em ação

Um exemplo de higiene cibernética embasada em análises seriam métricas como o tempo médio até o patch (MTTP) e o tempo médio até a correção (MTTR) das vulnerabilidades. Muitas organizações realizam um rastreamento de MTTP para assegurar-se de que estão abaixo de um limiar específico mês após mês. Isso respalda o cumprimento de qualquer mandato normativo que se aplique ao setor.

Outras métricas que se aplicam à higiene da TI poderiam ser os padrões de uso, a autenticação de credenciais e quem inicia a sessão e onde, o que também se aplica à segurança. O resultado final é resolver as vulnerabilidades e eliminar qualquer software dos pontos de extremidade que não cumpra ou supere as diretrizes estabelecidas.

A análise respalda alertas e valores de referência

Os alertas são uma das áreas que a Tanium está aproveitando a partir de sua associação com a Salesforce. É uma ferramenta de diagnóstico essencial que poupa tempo e dinheiro do departamento de TI.

Por exemplo, se um cliente da Tanium utiliza o Enforce ou o Performance Monitoring e surge um problema, semelhante à como se o consumo de CPU de uma máquina crítica estivesse fora dos gráficos, gera-se uma alerta que elimina a carga de TI para procurar problemas. A referência caminha de mãos dadas com os alertas porque os alertas precisam ter limiares.

Há várias formas de estabelecê-los. Um enfoque é imputar valores de referência “automáticos”. Se uma organização acredita que seu ambiente é relativamente saudável, o estado operacional atual é a referência.

Portanto, ela configura os alertas para informar ao departamento de TI quando algum indicador fugir ao previsto. Poderiam ser picos de CPU ou de memória ou uma versão de software modificada em um ponto de extremidade. A análise pode desempenhar um papel importante aqui ajudando as organizações a determinar se “normal” é o mesmo que saudável.

Realmente, tudo se reduz à configuração. Suas ferramentas devem dizer como é um ponto de extremidade saudável, e essa é a referência a tomar. Os alertas indicam quando ocorre algo que muda o estado de referência. Você precisa do tipo de dados que lhe facilite estabelecer limiares com uma margem razoável, o que permite certo desvio devido à atividade normal. Sem isso, você acabaria tendo uma “tempestade de alertas”, e as pessoas deixariam de lhes prestar atenção.

CONCLUSÃO

A análise de TI auxilia na tomada de decisões baseada em dados

A tomada de decisões baseada em dados (DDDM) é exatamente o que parece. A DDDM utiliza fatos, métricas e dados para guiar as decisões empresariais estratégicas harmonizadas com as metas, objetivos e prioridades. Se as organizações puderem aproveitar todo o valor de seus dados, todo o mundo estará capacitado para tomar melhores decisões.

As análises de TI e DDDM existem porque os executivos, com frequência, tomam decisões baseadas no ímpeto ou em pressentimentos. Às vezes, talvez dependendo do executivo e do contexto, os pressentimentos estão corretos. Por exemplo, Fred Smith tem uma visão do negócio do transporte e, apesar do ceticismo generalizado, cria a Federal Express. Michael Eisner ouve algo para um programa pouco convencional e, seguindo seu instinto, compromete-se a desenvolver "Quem quer ser milionário?"

Mas o instinto não é a forma como queremos que uma empresa opere de maneira consistente. Os dados são uma base bem mais confiável para a tomada de decisões.

Um enfoque moderno

O propósito deste e-book foi explicar a importância dos dados e das análises para obter uma boa higiene de TI, o que, por sua vez, melhora e respalda a posição de segurança de uma organização. Como explicamos, a análise baseada em dados em tempo real fornece informações válidas para a tomada de decisões empresariais imediatas, além de reparar as brechas existentes em visibilidade e resiliência. É um enfoque que beneficia as equipes de Operações e Segurança.

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

Tanium, única provedora do setor de gerenciamento convergente de endpoints (XEM), lidera a mudança de paradigma nos enfoques herdados para gerenciar ambientes complexos de segurança e tecnologia. Só a Tanium protege todas as equipes, endpoints e fluxos de trabalho das ameaças cibernéticas integrando TI, Operações, Segurança e Risco em uma única plataforma que oferece visibilidade integral em todos os dispositivos, um conjunto unificado de controles e uma taxonomia comum para um único propósito compartilhado: proteger as informações críticas e a infraestrutura em escala.

Visite-nos em www.tanium.com ou siga-nos no LinkedIn e Twitter.