WHITE PAPER

FireEye

POR DENTRO DAS VIOLAÇÕES DE DADOS:

Os dez maiores erros que os responsáveis pela resposta a incidentes cometem ao combater ameaças avançadas

SUMÁRIO

Introdução

Independente de trabalharem para uma nova empresa em ascensão ou para uma gigante do setor, as equipes de resposta a incidentes de segurança estão cada vez mais sob cerco. Os ataques cibernéticos de hoje são sofisticados, incansáveis e devastadores, custando às empresas dos EUA U$ 8,9 milhões por ano, em média[1]. Ao atacar em múltiplos estágios e por múltiplos vetores, as ameaças persistentes avançadas (APTs) e outros ataques sofisticados podem evitar facilmente a detecção com base em assinaturas e outras defesas tradicionais.

As estatísticas são alarmantes. Quase metade de todos os profissionais de segurança de TI entrevistados recentemente pelo Information Security Media Group (ISMG) informaram ter encontrado código malicioso no último ano que resultou em inatividade do sistema.[2] Além disso, cerca de dois terços têm dificuldades para detectar APTs: 62% têm problemas com a velocidade da detecção e 44% têm problemas com a precisão da detecção.

O que é ainda mais preocupante: apesar de sua sensação de insegurança cibernética, somente 28% das empresas têm um plano de resposta a incidentes para APTs. Um número ainda menor, apenas uma em cada cinco, considerou seus programas de resposta a incidentes como "muito eficazes".

Boas qualificações para gerenciamento de crises são raras. Nos momentos frenéticos após uma violação, erros cruciais podem prolongar um ataque e permitir mais danos. Esses erros tendem a ocorrer qualquer que seja o tamanho da organização, o escopo do incidente ou o nível técnico dos responsáveis pela resposta.

Respaldado pela ampla experiência da equipe do FireEye® Labs na linha de frente, este documento descreve os dez erros mais comuns, cinco estratégicos e cinco técnicos, cometidos pelas equipes de resposta a incidentes ao combater ataques. O documento também explica os efeitos desses erros e como evitá-los com um plano bem definido de resposta a incidentes.

Erros estratégicos

Os erros estratégicos são falhas no planejamento, na estrutura e na abordagem à segurança de TI. Essa categoria envolve decisões em nível executivo e respostas a incidentes no contexto dos maiores processos de negócios.

Nº 1: não determinar o escopo de um incidente

Para muitas organizações, responder a uma violação traz a sensação de uma batalha perdida. Elas têm dificuldade em detectar e identificar as localizações do malware e, por isso, não conseguem conter e reparar os danos de forma adequada. Na maioria dos casos, após um longo esforço para corrigir a violação, elas descobrem que estão novamente infectadas.

Ambos os cenários são sintomas do mesmo problema: a falta de uma compreensão clara da

[1] Ponemon Institute, "2012 Cost of Cyber Crime Study: United States" (Estudo sobre o custo do crime cibernético em 2012: Estados Unidos), outubro de 2012.

[2] Information Security Media Group, "2013 Incident Response Survey" (Pesquisa sobre a resposta a incidentes em 2013), julho de 2013.

ameaça. Muitas equipes de resposta a incidentes não compreendem quem são os elementos de ameaças, como estão atacando ou qual é o alvo.

Essa falta de conhecimento leva à criação de planos de contenção insuficientes e à atribuição de recursos inadequados para investigar as violações. Uma organização pode concentrar a segurança nas áreas erradas, por exemplo, ou investir nas qualificações erradas para as equipes de segurança de TI. Sem dedicar o tempo necessário para encontrar o "paciente zero" (a primeira máquina comprometida) e determinar como o malware se espalhou a partir dali, as equipes de resposta a incidentes não têm mais conhecimento ou resistência do que quando começaram.

Nº 2: processo inadequado para lidar com incidentes

Como a pesquisa do ISMG previamente citada revela, muitas organizações têm falhas no plano de resposta a incidentes, se é que possuem um plano. A maioria dos planos analisados pela FireEye estão desatualizados ou não foram testados, custando às organizações tempo e recursos preciosos quando ocorre uma violação.

Muitas vezes, o "plano" de resposta a incidentes de uma empresa é simplesmente apagar e recriar a máquina infectada. Além de destruir evidências que poderiam ser úteis, essa abordagem deixa as empresas vulneráveis ao mesmo ataque.

Todo plano de resposta deve ter os seguintes elementos, que são explicados em mais detalhes na seção "Recomendações":

- Identificação
- Classificação
- Determinação do nível de gravidade
- Comunicação
- Escalação
- Contenção
- Correção
- Geração de relatório

Nº 3: não envolver a liderança executiva

Embora os ataques cibernéticos possam ter graves implicações para os negócios, incluindo danos à sua marca, perda de dinheiro e de clientes, os líderes executivos raramente se envolvem no planejamento da resposta a incidentes ou supervisionam o processo após uma violação. Essa falha crucial agrava o incidente.

Sem um líder executivo no comando, o peso do processo de tomada de decisões fica todo sobre a equipe de segurança da organização, que tende a se concentrar mais nos aspectos técnicos do ataque e a não levar em conta os impactos de suas decisões sobre os negócios. Os profissionais de segurança trabalham para corrigir o problema técnico, o que muitas vezes resulta em uma resposta incompleta, e não levam em consideração o que o problema significa para o negócio como um todo.

Caso em questão: a FireEye tem visto equipes de resposta a incidentes desativando o servidor do Exchange da companhia durante um período de negócios crucial, em um esforço mal orientado para conter e investigar uma violação. Um líder executivo teria considerado o impacto de uma medida tão drástica sobre os negócios e pesaria melhor as necessidades da empresa em relação aos requisitos técnicos da resposta ao incidente.

Em um ambiente em que a propriedade intelectual e os dados dos clientes estão entre os ativos mais valiosos da empresa, os líderes executivos podem oferecer um contexto muito necessário e equilíbrio ao responder a uma violação, avaliando seu impacto sobre os negócios.

E se o ataque se espalhar além da organização para sua cadeia de suprimentos e outros parceiros, a liderança executiva precisa decidir se deve envolver uma consultoria externa ou convocar reuniões de emergência da diretoria, decisões que estão muito além do escopo da equipe de segurança.

Nº 2: processo inadequado para lidar com incidentes

Como a pesquisa do ISMG previamente citada revela, muitas organizações têm falhas no plano de resposta a incidentes, se é que possuem um plano. A maioria dos planos analisados pela FireEye estão desatualizados ou não foram testados, custando às organizações tempo e recursos preciosos quando ocorre uma violação.

Muitas vezes, o "plano" de resposta a incidentes de uma empresa é simplesmente apagar e recriar a máquina infectada. Além de destruir evidências que poderiam ser úteis, essa abordagem deixa as empresas vulneráveis ao mesmo ataque.

Todo plano de resposta deve ter os seguintes elementos, que são explicados em mais detalhes na seção "Recomendações":

- Identificação
- Classificação
- Determinação do nível de gravidade
- Comunicação
- Escalação
- Contenção
- Correção
- Geração de relatório

Nº 3: não envolver a liderança executiva

Embora os ataques cibernéticos possam ter graves implicações para os negócios, incluindo danos à sua marca, perda de dinheiro e de clientes, os líderes executivos raramente se envolvem no planejamento da resposta a incidentes ou supervisionam o processo após uma violação. Essa falha crucial agrava o incidente.

Sem um líder executivo no comando, o peso do processo de tomada de decisões fica todo sobre a equipe de segurança da organização, que tende a se concentrar mais nos aspectos técnicos do ataque e a não levar em conta os impactos de suas decisões sobre os negócios. Os profissionais de segurança trabalham para corrigir o problema técnico, o que muitas vezes resulta em uma resposta incompleta, e não levam em consideração o que o problema significa para o negócio como um todo.

Caso em questão: a FireEye tem visto equipes de resposta a incidentes desativando o servidor do Exchange da companhia durante um período de negócios crucial, em um esforço mal orientado para conter e investigar uma violação. Um líder executivo teria considerado o impacto de uma medida tão drástica sobre os negócios e pesaria melhor as necessidades da empresa em relação aos requisitos técnicos da resposta ao incidente.

Em um ambiente em que a propriedade intelectual e os dados dos clientes estão entre os ativos mais valiosos da empresa, os líderes executivos podem oferecer um contexto muito necessário e equilíbrio ao responder a uma violação, avaliando seu impacto sobre os negócios.

E se o ataque se espalhar além da organização para sua cadeia de suprimentos e outros parceiros, a liderança executiva precisa decidir se deve envolver uma consultoria externa ou convocar reuniões de emergência da diretoria, decisões que estão muito além do escopo da equipe de segurança.

Nº 4: não considerar os aspectos jurídicos

Outro motivo para envolver os líderes executivos: o impacto jurídico de uma violação e da resposta. Em todo o mundo, os governos estabeleceram leis de notificação e divulgação para proteger empresas e consumidores, caso ocorra uma violação. Essas leis podem ser complicadas, dependendo do país e do setor. Em muitos casos, uma violação também significa estabelecer comunicação com representantes da lei ou de agências reguladoras.

Na urgência de conter uma violação, muitos responsáveis pela resposta a incidentes frequentemente menosprezam as implicações de conformidade, de notificação e jurídicas de uma violação de dados. Mas com o risco à privacidade dos clientes e uma possível responsabilidade civil, as questões da cadeia de custódia não podem ser deixadas em segundo plano. Um plano de resposta a incidentes que não considera as questões jurídicas pode criar problemas que se estendem muito além da própria violação.

A maioria das empresas estão cientes de suas obrigações nessas áreas, especialmente aquelas em setores muito regulados, governados pela Food and Drug Administration (FDA), pelo Health Insurance Portability and Accountability Act (HIPAA), pela Securities and Exchange Commission (SEC) ou pelo PCI Security Standards Council. Isso também vale para as agências do governo sujeitas ao Federal Information Security Management Act (FISMA), administrado pelo National Institute of Standards and Technology (NIST). Porém, com frequência, as empresas que formam a cadeia de suprimento desses setores não consideram suas responsabilidades sob as mesmas regras. Os responsáveis pela resposta

a incidentes devem compreender como a violação afeta não só a organização visada, mas também seus parceiros, fornecedores e outros interessados.

Mesmo quando uma empresa reconhece esses requisitos, é comum adiá-los até que a violação tenha sido contida e solucionada, quando é tarde demais para corrigir quaisquer problemas no modo como a equipe tratou e preservou as evidências ao longo do processo. Em vez disso, as organizações devem integrar os aspectos jurídicos de uma violação à resposta a incidentes, desde o início. O plano de resposta a incidentes deve definir como a organização irá tratar as evidências, documentar os procedimentos e notificar prontamente os interessados apropriados.

Nº 5: não se comunicar

A comunicação é sempre importante e absolutamente crucial no cenário de muita pressão e desdobramentos rápidos de uma violação de dados. Se os responsáveis pela resposta a incidentes não se comunicam uns com os outros e com a gerência, a situação pode piorar rapidamente.

O ponto mais importante de uma boa comunicação durante uma violação é uma reunião diária e obrigatória sobre o status da situação, que deve incluir todas as equipes cruciais envolvidas na resposta ao incidente. Essa reunião é especialmente essencial para as equipes que trabalham em turnos.

A reunião de status também serve como uma reunião de transferência para coordenar os esforços. As organizações também devem notificar os usuários finais sobre a resposta ao incidente quando for apropriado, incluindo as responsabilidades desses usuários e como a resposta ao incidente pode afetá-los. Por exemplo, digamos que a equipe de resposta a incidentes precise realizar uma análise forense no computador de um usuário específico. Informar antecipadamente ao usuário daquela máquina pode minimizar a interrupção do trabalho.

Embora uma comunicação aberta seja vital para a resposta a incidentes, o contrário também é

igualmente importante. As empresas devem controlar rigidamente quais informações serão transmitidas e para quem, além de garantir que todas as comunicações sejam seguras.

Erros técnicos

Os erros técnicos são falhas na execução das atividades da equipe de segurança de TI de uma empresa ao se preparar e ao responder a uma violação. Sem o conhecimento técnico requerido para descobrir, analisar e remover as ameaças avançadas de hoje, até as melhores estratégias falharão.

Nº 1: não compreender a mecânica da ameaça

O erro estratégico de não avaliar o escopo completo de um incidente, mencionado previamente neste documento, tem uma contraparte: o erro técnico de não compreender os detalhes operacionais da própria ameaça.

As empresas tendem a subestimar o impacto de uma violação, sem compreender totalmente o escopo completo do incidente ou quais pontos de entrada foram comprometidos.

Para localizar malware avançado em um sistema, é necessário saber as respostas para as seguintes perguntas:

- **Como o malware sobrevive a uma reinicialização?** Essa capacidade ajuda o malware a estabelecer uma persistência em máquinas individuais.
- **Como o malware se move lateralmente no seu ambiente de TI?** Essa capacidade ajuda a fazer o reconhecimento, a localizar os itens valiosos da organização e a estabelecer persistência na rede.
- **Como o malware se comunica além da sua rede?** Essa capacidade permite que o malware possa receber instruções de servidores de comando e controle (CnC) e vazar dados valiosos.
- **Quais são os estágios típicos das APTs?** Os múltiplos estágios de uma APT tornam mais difícil detectála e bloqueá-la.
- **Como o malware explora vulnerabilidades no sistema atacado?** Detectar a exploração inicial é essencial, porque os estágios subsequentes do ataque geralmente são criptografados ou obscurecidos.

A menos que uma empresa gaste tempo suficiente analisando um ataque, as respostas provavelmente serão incorretas ou inexistentes. E as conclusões erradas geralmente levam a contramedidas inadequadas e ao fracasso em conter e corrigir de fato a ameaça.

Nº 2: conhecimento incompleto da infraestrutura

Você jamais contrataria guarda-costas sem dizer a eles quem deve ser protegido. Apesar disso, muitas empresas usam essa abordagem à segurança de TI.

Com frequência, os responsáveis pela resposta a incidentes têm um layout desatualizado ou incompleto de suas redes. Eles não identificaram seus ativos mais valiosos, onde os ativos essenciais estão localizados ou quais atividades são regularmente registradas no sistema.

No clima frenético dos negócios de hoje, nem sempre é fácil manter essas informações atualizadas. O crescimento, fusões, aquisições e as mudanças constantes da tecnologia significam um fluxo constante para a infraestrutura das organizações. Para complicar mais as coisas, muitas empresas terceirizam funções de TI e de segurança e usam cadeias de suprimentos estritamente interconectadas. Isso requer comunicação e correlação ainda melhores, de

modo que os principais integrantes da equipe de resposta a incidentes tenham uma imagem precisa da infraestrutura e saibam quem é responsável por cada parte diferente dela.

Por exemplo, suponha que uma companhia terceirize seu suporte e o fornecedor desse serviço, por sua vez, terceirize suas operações de TI. Mapear o sistema e as várias funções e responsabilidades das equipes envolvidas em cada componente se torna especialmente complicado.

Essa complexidade torna ainda mais vital ter uma compreensão completa dos pontos de presença da sua organização, da localização de dados confidenciais e da infraestrutura terceirizada.

Nº 3: não monitorar o tráfego interno da rede

Na maioria dos casos, o malware se move lateralmente entre os sistemas de TI para alcançar um alvo específico, após penetrar as defesas externas da rede da empresa. A menos que você saiba o que está trafegando pela sua rede, o seu sistema é como um ovo quente para os atacantes: uma casca dura com um interior delicado.

Infelizmente, poucas organizações têm capacidades adequadas de captura de rede para monitorar as atividades na rede, o que as deixa cegas para o movimento do malware dentro de suas próprias redes.

Monitorar a atividade no perímetro da sua rede é sempre importante. Mas isso não é suficiente contra as ameaças avançadas de hoje. O monitoramento interno é essencial.

Nº 4: não registrar

Nenhuma empresa gosta de registrar o tráfego da rede e outras atividades de TI. Muitas vezes considerada como uma tarefa ingrata, a geração de registros é, por tradição, trabalhosa, cara e, até que ocorra uma violação, de baixa prioridade.

Mas sem esses registros, uma análise forense detalhada é difícil, se não impossível. Os investigadores simplesmente não têm coisa alguma para examinar: nenhuma trilha de pistas para seguir, nenhum padrão comportamental para analisar, nenhuma linha do tempo para reconstruir. Quando se trata de resposta a incidentes, a geração de registros é um requisito fundamental.

A boa notícia é que essa tarefa está se tornando mais fácil e econômica. As ferramentas modernas de geração de registros facilitam a implementação de registros centralizados. Além disso, o custo por byte do armazenamento de dados continua a despencar. Hoje, os profissionais de segurança têm menos dificuldades com essa tarefa vital. As ferramentas avançadas de gerenciamento de eventos e informações de segurança não só podem agregar os registros do seu sistema como também ajudam a correlacionar informações coletadas por uma gama de ferramentas de segurança no seu arsenal.

Nº 5: não aproveitar ferramentas existentes

A sua organização pode realmente priorizar a segurança de TI e até respaldar esse compromisso com os sistemas de defesa cibernética mais sofisticados e modernos do mercado. Porém, a menos que esses sistemas sejam implementados de forma efetiva, nem mesmo as defesas de segurança mais modernas irão fortalecer a sua resposta a incidentes.

Muitas organizações possuem ferramentas de segurança implementadas, incluindo a plataforma FireEye. Mas a falta de treinamento e de gerenciamento prejudica sua capacidade defensiva. Ao trabalhar com clientes no local para otimizar seus sistemas de segurança, a FireEye frequentemente encontra uma integração inadequada das ferramentas existentes de segurança do cliente, como firewalls, sistemas de proteção contra intrusão de rede, proteção contra intrusão com base em hosts, software antivírus

(AV) e outros sistemas. Por exemplo, uma ferramenta de rede pode não se comunicar com a segurança baseada em terminal. Ou uma ferramenta de geração de registros pode não estar configurada para identificar a disseminação lateral do malware.

Recomendações

A melhor forma de evitar esses dez erros comuns é ter um plano robusto e testado de resposta a incidentes. Toda organização deve ter um plano com um fluxo de trabalho claro e consistente. Esse plano deve ter funções claramente definidas, uma estratégia abrangente de comunicação e o envolvimento do nível executivo, a fim de obter uma visão completa das ameaças cibernéticas e dos possíveis impactos jurídicos e de negócios de uma violação.

Ao mesmo tempo, as equipes de resposta a incidentes devem compreender todo o escopo da ameaça, tanto de uma perspectiva técnica como de negócios. Elas devem documentar sua infraestrutura de TI e saber onde estão seus ativos mais essenciais. E elas devem aproveitar as ferramentas já implementadas para monitorar o tráfego externo e interno, manter registros de atividade detalhados e garantir que os componentes individuais de seus sistemas de defesa funcionem juntos como um todo integrado.

A FireEye recomenda um plano de resposta a incidentes com os seguintes elementos, explicados nas seções correspondentes:

- Identificação
- Classificação
- Determinação do nível de gravidade
- Comunicação
- Escalação
- Contenção
- Correção
- Geração de relatório

Identificação

A identificação é a capacidade da equipe de segurança de identificar de forma rápida e precisa um evento de segurança, desde o primeiro indicador de comprometimento. Isso requer controles de segurança competentes e uma capacidade de monitoramento madura.

Classificação

Quando um evento de segurança ocorre, deve ser classificado como um de vários tipos de eventos. Para garantir que os eventos sejam categorizados de maneira consistente, certifique-se de que todos compreendam e reconheçam essas categorias. Recomendamos não mais do que dez tipos de eventos.

Os seguintes exemplos, que classificam os incidentes pelo vetor de ataque, foram obtidos do National Institute of Standards and Technology[3]:

- Mídia externa/removível
- Atrito
- Roubo ou perda de ativos digitais
- E-mail
- Uso impróprio
- Roubo ou perda de equipamento
- Outros

[3] NIST, "Computer Security Incident Handling Guide" (Guia de tratamento de incidentes de segurança em informática), agosto de 2012.

Determinação do nível de gravidade

Uma vez que o evento tenha sido identificado e classificado, é necessário atribuir um nível de gravidade. Essa etapa determina os canais apropriados de comunicação e escalação.

Recomendamos não mais do que cinco níveis de gravidade. Eis alguns exemplos:

- Investigação (azul): nível 0
- Baixo (amarelo): nível 1
- Elevado (laranja): nível 2
- Grave (vermelho): nível 3

Comunicação

A comunicação é a espinha dorsal do planejamento da resposta a incidentes. O plano de comunicação normalmente é dividido em duas áreas: interna e externa.

A comunicação interna lida com duas questões: quem da organização será notificado durante um incidente de segurança e como essas pessoas serão notificadas. A resposta depende do tipo de incidente e do nível de gravidade. Recomendamos a criação de um fluxograma de comunicação para cada tipo de incidente e nível de gravidade. Além disso, estabeleça regras para controlar quem se comunica com quem durante um incidente para garantir que todas as informações circulem somente entre as pessoas que precisam delas.

A comunicação externa lida com a troca de informações sobre o incidente com outras organizações. Essas entidades podem incluir fornecedores, contratados, representantes da lei, agências de mídia, grupos reguladores, empresas de advocacia e outras. As organizações devem controlar estritamente todas as comunicações externas. A FireEye recomenda que todas as comunicações externas sejam encaminhadas por especialistas das áreas de marketing, relações públicas, jurídica e assim por diante. Não permita que os responsáveis pela resposta a incidentes comuniquem-se diretamente com grupos externos sem a supervisão da equipe de comunicações externas.

Escalação

A escalação é um processo predefinido e formal de comunicação e resposta que estabelece como notificar e acionar os responsáveis pela resposta a incidentes. O plano de escalação é sempre baseado no tipo de incidente e no nível de gravidade. Por exemplo, cada plano deve identificar quando a equipe de resposta a incidentes de segurança de informática (CSIRT) será acionada. O objetivo é garantir que os recursos apropriados, como o número adequado de pessoas com as qualificações necessárias, serão mobilizados para responder a um incidente.

Contenção

A contenção se refere às contramedidas de segurança para deter uma ameaça imediata. Ela é sempre focada em deter a ameaça e não em corrigir os danos. Por exemplo, se um incidente envolve uma grave infecção por malware, a contenção é o esforço necessário para identificar a ameaça, impedir a sua disseminação e garantir que o malware não possa fazer comunicações de saída.

Correção

A correção se refere à restauração dos sistemas e serviços para o estado anterior ao incidente e à implementação de contramedidas a longo prazo para evitar ataques similares no futuro. Com o malware tradicional, a contenção e a correção podem ser combinadas em um processo misto. Mas o malware avançado é muito mais sofisticado

e os elementos de ameaças de hoje normalmente se incorporam na sua organização. É por isso que a FireEye recomenda uma abordagem em duas fases para a resposta a incidentes: primeiro, foque na contenção e, depois, na correção.

Geração de relatório

A geração de relatórios é a fase final de uma resposta a incidentes. Ela envolve a criação de um relatório detalhado sobre o incidente para uso interno, além das notificações e relatórios externos requeridos por regras normativas ou específicas do setor. Use a fase de geração de relatórios para reavaliar o plano de resposta a incidentes. Faça uma análise após o fato e defina e implemente as melhorias ou alterações necessárias.

Conclusão

No panorama de ameaças de hoje, os ataques cibernéticos são inevitáveis. Os elementos de ameaças estão visando a sua empresa, seus ataques estão mais sofisticados e o modo como você responde ao dilúvio crescente de incidentes nunca foi tão crucial. Evitar erros técnicos e estratégicos importantes pode ser a diferença entre deter os ataques com sucesso ou se transformar na próxima manchete.

Para ter uma resposta a incidentes bem informada, as empresas precisam de um processo eficiente e das ferramentas certas, a fim de compreender totalmente e responder aos ataques de forma precisa e em tempo hábil. Para saber como a FireEye pode ajudar a sua organização a fortalecer seu plano de resposta a incidentes, visite o nosso site: http://www.fireeye.com/products-and-solutions/threat-protection-platform.html.

Sobre a FireEye

A FireEye inventou uma plataforma de segurança de finalidade específica, com base em máquina virtual, que proporciona proteção em tempo real para corporações e governos do mundo todo contra a próxima geração de ataques cibernéticos. Esses ataques cibernéticos altamente sofisticados contornam facilmente defesas tradicionais com base em assinaturas, como gateways, antivírus, sistemas de prevenção de intrusões e firewalls de próxima geração. A plataforma FireEye proporciona proteção dinâmica e em tempo real contra ameaças, sem utilizar assinaturas, para proteger as organizações nos principais vetores de ameaças, incluindo Web, e-mail e arquivos, e nos diversos estágios do ciclo de vida de um ataque. O núcleo da plataforma FireEye é um mecanismo de execução virtual, complementado pela inteligência dinâmica sobre ameaças, para identificar e bloquear ataques cibernéticos em tempo real. A FireEye tem mais de 1.000 clientes em mais de 40 países, incluindo mais de um terço das empresas da Fortune 100.

Sobre a First Tech

A First Tech é uma provedora de soluções e serviços de tecnologia e há mais de 21 anos atua no desenvolvimento e implantação de projetos de infraestrutura de voz, dados, videoconferência e segurança da informação.

A First Tech atua em parceria com a FireEye para detectar ataques cibernéticos e como eles acontecem, entendendo os riscos que representam para os ativos mais valiosos e ajudando empresas a solucionarem incidentes de segurança rapidamente.

Acesse: www.first-tech.com

FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | 408.321.6300 | 877.FIREEYE (347.3393) | LATAM@fireeye.com | **www.fireeye.com**