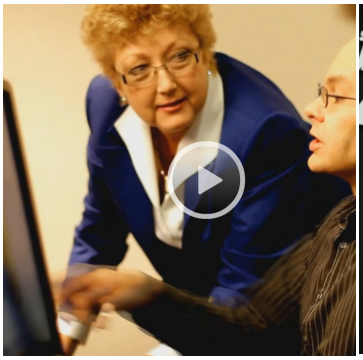
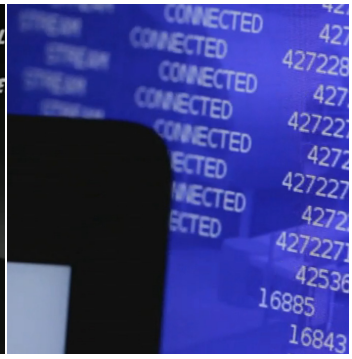
As iniciativas de segurança cibernética de Michigan reduzem os riscos com melhor treinamento dos funcionários





RESUMO EXECUTIVO

Objetivos

- Reduzir os riscos à segurança contando com moradores e funcionários mais bem treinados
- Trabalhar em conjunto com o setor privado em relação a infraestrutura crítica e segurança cibernética
- Criar oportunidades de segurança e educação contínuas

Estratégia

- Trabalhar em conjunto com a Polícia Estadual de Michigan e outros parceiros governamentais responsáveis pelo gerenciamento de emergências em todo o estado

Soluções

- Treinamento em grupo e online para funcionários do estado
- O Cyber Range, que permite que a equipe tecnológica pratique exercícios de segurança de dados
- Uma estratégia de resposta à interrupção cibernética, formada em colaboração com entidades públicas e privadas para responder à possibilidade de ataque cibernético em grande escala

Impacto

- Conquista da nota "A" no 2012 Digital States Awards da NASCIO, sendo um dos dois únicos estados tão premiados
- Moradores e funcionários mais bem treinados; riscos à segurança reduzidos
- Várias ameaças cibernéticas graves evitadas; diminuição de danos decorrentes de tentativas de phishing e malware
- ROI estimado do programa: mais de 100:1
- Novas oportunidades de segurança e educação contínuas

Informações básicas

Em janeiro de 2014, a Cisco divulgou os resultados de uma análise profunda dos benefícios econômicos da Internet de Todas as Coisas (IoE) para o setor público. O modelo da Cisco revelou que a adoção dos recursos de IoE em 40 casos de uso fundamentais do setor público para os próximos 10 anos, como água inteligente, edifícios inteligentes, energia inteligente, estacionamento inteligente e muito mais, resultaria em cerca de US$ 4,6 trilhões de "valor em jogo" (http://bit.ly/1aSGlzn).

Na próxima fase de sua análise, a Cisco contratou o Cicero Group, uma firma líder do setor de consultoria e pesquisas estratégicas voltadas para dados, para realizar um estudo global dos recursos de IoE nesses 40 casos de uso. A intenção era descobrir como as melhores empresas do setor público "conectam o que antes funcionava de maneira independente", conforme a definição da Cisco. Para isso, o Cicero Group realizou entrevistas com várias jurisdições líderes do setor público: governos federal, estadual e municipal; empresas da área de saúde; instituições de ensino; e organizações não governamentais (ONGs); para analisar como esses líderes globais tiram proveito da IoE atualmente.

A pesquisa examinou projetos reais, que são gerados em escala (ou através de pilotos com potencial óbvio de escala) e que representam a vanguarda da preparação e da maturidade da IoE no setor público. O objetivo da pesquisa era entender o que havia mudado nas jurisdições em termos de pessoas, processos, dados e coisas e como outras empresas do setor público podem aprender (e replicar) com o caminho trilhado por esses líderes globais de IoE. Em muitos casos, essas jurisdições são clientes da Cisco; em outros, não. O foco desses perfis de jurisdição, portanto, não é elogiar o papel da Cisco no sucesso dessas empresas, mas documentar a excelência da IoE e o modo como as entidades do setor público colocam a IoE em prática atualmente, além de informar um roadmap de mudanças que permitirá que o setor público enfrente desafios complexos em várias frentes usando as melhores práticas do mundo.

Sobre o Estado de Michigan

O Estado de Michigan implementou uma série de iniciativas de segurança cibernética que o colocam entre os principais estados dos EUA em relação a educação e conscientização da segurança de dados. Essas iniciativas incluem um programa de treinamento de funcionários inovador e divertido, o Cyber Range, no qual os especialistas técnicos aprendem a combater ameaças à segurança, além de colaboração público-privada para a criação da Estratégia de resposta ao ataque cibernético de Michigan, uma estratégia de resposta a guerra cibernética.

Dan Lohrmann é diretor de segurança (CSO), diretor de segurança da informação (CISO) e diretor-adjunto de segurança cibernética e proteção à infraestrutura do Departamento de Tecnologia, Gestão e Orçamento (DTMB) de Michigan. O Sr. Lohrmann trabalhou em diversas funções de liderança e segurança no setor público, inclusive na Agência de Segurança Nacional (NSA). Ele foi diretor de segurança da informação (CISO) e diretor de tecnologia (CTO) de Michigan antes de assumir o seu cargo atual.

O Estado de Michigan implementou uma série de iniciativas de segurança cibernética que o colocam entre os principais estados dos EUA em relação a educação e conscientização da segurança de dados.

Andris Ozols é analista e consultor sênior de políticas do Departamento de Tecnologia da Informação do Estado de Michigan. Ele tem mais de 42 anos de experiência como funcionário público de Michigan.

Objetivos

O principal objetivo das iniciativas de segurança cibernética de Michigan era reduzir os riscos à segurança contando com moradores e funcionários mais bem treinados. O estado também procurava coordenar com o setor privado em relação a infraestrutura crítica e segurança cibernética e criar oportunidades de segurança e educação contínuas.

Estratégia

O diretor executivo de segurança do Estado de Michigan e o Departamento de Tecnologia, Gestão e Orçamento de Michigan são responsáveis pela manutenção e administração gerais da implementação do plano de iniciativas de segurança cibernética do estado. Estes esforços são coordenados com a Polícia Estadual de Michigan e outros parceiros governamentais responsáveis pelo gerenciamento de emergências em todo o estado.

A maior parte do financiamento para iniciativas de segurança cibernética de Michigan é pública, proveniente de várias fontes federais e estaduais. Isso inclui subsídios do Departamento de Segurança Nacional e recursos disponibilizados mediante a colaboração com entidades de ensino superior.

- Cyber Summits e Breakfast Conference são eventos autossuficientes que se mantêm com patrocínios e taxas de participação.
- O programa de treinamento online Security Mentor foi elaborado por menos de US$ 200.000, com um custo estimado por funcionário de cerca de 30 centavos por lição durante um período de dois anos.
- O Michigan Cyber Range foi criado com o auxílio de US$ 2 milhões em subsídios e doações privadas, com um adicional de 20% do financiamento total fornecido por fontes do governo. Espera-se que o governo do estado economize de 40 a 50% em certificação, curso e despesas de viagem com o uso do programa.

Solução

Como diretor de segurança de Michigan, em cooperação com o Governador de Michigan Rick Snyder, o Sr. Lohrmann supervisiona o programa de segurança cibernética do estado, a Michigan Cyber Initiative. Os componentes incluem treinamento em grupo e online para funcionários do estado; uma configuração "Cyber Range" que permite que a equipe tecnológica pratique exercícios de segurança de dados; e uma estratégia contra o ataque cibernético, formada em colaboração com entidades públicas e privadas (como grandes empregadores, serviços de utilidade pública e agências federais) para responder à possibilidade de um ataque cibernético em grande escala.

Treinamento público de funcionários

O programa de treinamento online sobre segurança cibernética realizado pelo estado a cada dois meses é a base do seu sistema de treinamento de funcionários. O Sr. Lohrmann também coordena os eventos Security Summits e Breakfast Conference Series e publica um boletim informativo mensal.

No início do programa de treinamento online, o Sr. Lohrmann entrevistou os funcionários para determinar a eficácia do programa atual, que consistia basicamente no envio de e-mails contendo hyperlinks para vídeos sobre informações de segurança. Os resultados não foram encorajadores.

"Nos últimos 12 meses, passamos de cerca de 10% de funcionários estaduais em treinamento para bem mais de 90%. Ficamos maravilhados com o número de pessoas que fizeram o treinamento."

Dan Lohrmann,

Diretor de segurança (CSO), Diretor de segurança da informação (CISO) e Diretor-adjunto de segurança cibernética e proteção à infraestrutura do

Departamento de Tecnologia, Gestão e Orçamento de Michigan

O Sr. Lohrmann recorda: "Em alguns estudos de teste, as pessoas iniciavam os vídeos, iam até a cozinha, pegavam uma xícara de café, iam ao banheiro, voltavam, falavam sobre o jogo de ontem à noite e se relaxavam. Eles não estavam sequer assistindo aos vídeos. Isso não era bom. Queríamos interatividade. Queríamos que as pessoas realmente se envolvessem com o treinamento e, acima de tudo, queríamos mudar o comportamento delas. Não bastava marcar a caixa de seleção e dizer: "Sim, eu fiz o treinamento de segurança cibernética."

Para encontrar a melhor forma de atrair os funcionários do estado, o Sr. Lohrmann fez uma segunda pesquisa. "Montamos uma equipe para descobrir o que as pessoas queriam no treinamento. Elas disseram que queriam que fosse rápido. Não queriam um treinamento de duas ou até quatro horas de duração em frente ao computador. As pessoas queriam que ele fosse breve, mas frequente. Queriam que ele fosse atualizado regularmente. Queriam que ele fosse interessante. Queriam que ele fosse divertido."

O Sr. Lohrmann disse que o DTMB emitiu uma solicitação de proposta (RFP, Request for Proposal) para uma experiência de treinamento mais interativa, desafiando os fornecedores com a pergunta: "Como podemos mudar comportamentos e ter métricas para avaliar isso?"

O DTMB selecionou um programa de fornecedor que usava jogos e atividades interativas para promover comportamentos seguros em uma série de configurações. O programa foi implantado para todos os funcionários do estado ao longo de seis meses, com excelente resposta e feedback positivo. "Nos últimos 12 meses, passamos de cerca de 10% de funcionários do estado em treinamento para bem mais de 90%. Ficamos maravilhados com o número de pessoas que fizeram o treinamento."

"O mais surpreendente é que o feedback foi simplesmente fantástico", continuou o Sr. Lohrmann. "As pessoas disseram: "Nós adoramos! É a melhor coisa que o departamento de tecnologia já produziu." E recebemos comentários singulares, como: "Isso é incrível! Posso levar para casa? Posso mostrar para minha família? Posso usá-lo com os meus filhos?" Depois de cada lição, elas atribuem uma nota de 1 a 5, sendo 5 incrível e 1 nada agradável. Com 50.000 funcionários do estado, estamos com uma média de 4, o que é inédito nessa área."

O Sr. Lohrmann explicou o apelo dos exercícios de treinamento típicos: "Um dos jogos que eu mais gostei aborda a importância do papel de cada um no escritório, ensinando os funcionários a perceberem violações de segurança como, por exemplo, deixar documentos confidenciais em cima da mesa. Em seguida, o jogo pede que você classifique por que algo era uma violação de política ou uma violação de segurança". Outro jogo envolve um personagem, parecido como o Super Mario, que percorre um aeroporto procurando por 12 laptops perdidos ou roubados. "É uma contagem regressiva: você tem 90 segundos", explicou o Sr. Lohrmann. "Na primeira vez que joguei, acho que encontrei sete dos 12."

O Sr. Lohrmann disse que o aspecto mais importante do treinamento é a sua natureza altamente memorável. "A ideia é mudar comportamentos. Quando eu entro em aeroportos agora, não consigo parar de pensar nesse jogo do Super Mario", disse ele. "Não importa se você está no balcão de atendimento ou no portão de acesso, acaba pensando nisso. Os funcionários simplesmente adoraram. As pessoas dizem que ficam ansiosas para fazer as lições."

"O objetivo era fazer uma parceria público-privada, trazer universidades e parceiros federais para ajudar a determinar como nos preparamos para defender nossas redes e nossos sistemas contra os melhores e mais brilhantes do mundo."

Dan Lohrmann,

Diretor de segurança (CSO), Diretor de segurança da informação (CISO) e Diretor-adjunto de segurança cibernética e proteção à infraestrutura do

Departamento de Tecnologia, Gestão e Orçamento de Michigan

Michigan Cyber Range

Em um esforço para oferecer mais treinamento técnico à equipe de TI, o Sr. Lohrmann procurou recriar um ambiente de testes de segurança cibernética semelhante aos utilizados durante seu período na NSA. "A ideia era montar uma empresa e um treinamento, que chamamos de Michigan Cyber Range", explicou ele. "O Cyber Range fornece um local para testar, treinar, aprender e crescer em um ambiente não classificado. O objetivo era fazer uma parceria público-privada, trazer universidades e parceiros federais para ajudar a determinar como nos preparamos para defender nossas redes e nossos sistemas contra os melhores e mais brilhantes do mundo."

Segundo o Sr. Lohrmann, o Cyber Range oferece treinamento técnico sobre tópicos como hacking ético e diferentes tipos de perícia por cerca de metade do custo de enviar alguém para fora do estado para participar de um treinamento semelhante.

O Sr. Ozols também enfatizou a ampla abordagem no planejamento, dizendo: "De forma consciente e deliberada, adotamos uma perspectiva estadual trabalhando com entidades e governos locais. É igualmente uma parte da nossa responsabilidade na nossa visão e em nossos objetivos". Agora os especialistas em segurança cibernética de todo o estado e de todo o centro-oeste usam o site regularmente, inclusive a Guarda Nacional.

O Sr. Lohrmann disse que primeiro ele levou a ideia de um site com testes de habilidades cibernéticas ao Governador Snyder, que apoiou totalmente o projeto. O Sr. Lohrmann contratou uma firma de software para desenvolver a plataforma de teste: um sistema isolado logicamente e não classificado que permite que as equipes técnicas aprendam técnicas de segurança de dados por meio de uma série de exercícios.

As equipes técnicas do Sr. Lohrmann praticam habilidades com vários cenários de simulação, como "Alphaville", que o Sr. Lohrmann descreveu como uma "pequena cidade". Ele continuou: "Tem uma biblioteca, uma central de produção de energia, uma estação de tratamento de água e uma prefeitura. Você realmente pode invadi-las e defendê-las". Os funcionários do governo aprovados nos cursos se qualificam para várias certificações.

Estratégia de resposta ao ataque cibernético de Michigan

Segundo o Sr. Lohrmann, o Governador Snyder é um grande defensor da segurança cibernética. “Ele enfatizou que a guerra cibernética é a maior ameaça que os Estados Unidos enfrentam atualmente... A guerra nuclear pode ser a nº 1, mas, segundo ele, a cibernética é a ameaça mais provável, porque já está acontecendo.”

Em um esforço para criar uma estratégia de segurança em todo o estado, o Sr. Lohrmann formou uma coalizão de planejamento com representantes de interesses públicos essenciais e grandes empregadores em todo o estado. “Fazemos reuniões mensais e temos representantes das principais empresas privadas do setor em Michigan”, explicou o Sr. Lohrmann. “Temos a Consumers Energy, a DTE Energy e alguns bancos. Também temos alguns fornecedores de autopeças e outras grandes empresas de Michigan. Trabalhamos juntos para elaborar a estratégia de resposta em relação à forma como compartilhar informações sobre ameaças cibernéticas. Como trabalhamos juntos em caso de emergência? Como declaramos uma emergência? Quem vai telefonar? Como vamos coordenar?”

Em um esforço para criar uma estratégia de segurança em todo o estado, o Sr. Lohrmann formou uma coalizão de planejamento com representantes de interesses públicos essenciais e grandes empregadores em todo o estado.

O grupo publica suas conclusões online, na Estratégia de resposta ao ataque cibernético de Michigan, que foi considerada a melhor prática nacional pelo Departamento de Segurança Nacional.

“Não se trata apenas de divulgação e treinamento”, disse o Sr. Lohrmann. “O conceito por trás disso é muito novo. Historicamente, os governos estaduais respondem por incêndios, enchentes, tornados, emergências. O que temos agora são possíveis emergências cibernéticas. Nossa Estratégia contra o ataque cibernético nasceu do desejo de nos prepararmos para uma guerra cibernética que atinja todo o estado. E se a rede cair? Como vamos manter comunicação antes, durante e depois de um evento? Como trabalhamos em conjunto com o setor privado?” A estratégia também inclui políticas sobre compartilhamento de informações de ameaças cibernéticas, como definir uma emergência e uma lista de contatos de emergência.

As equipes técnicas do Sr. Ozols observou: “Somos um dos primeiros estados a analisar as oportunidades de desenvolvimento econômico e o emprego na indústria relacionados à segurança cibernética. Falamos com vários parceiros em potencial, como Canadá, Israel, etc. Isso também faz parte da divulgação. Faz parte do fato de que temos mais do que uma perspectiva de vida departamental, temos uma perspectiva estadual”.

Figura 1. Estado de Michigan: conexões novas e melhores.

Fonte: Cisco Consulting Services, 2014

Impacto

As iniciativas de segurança cibernética de Michigan conquistaram para o estado a nota “A” no 2012 Digital States Awards da Center for Digital Government, sendo um dos dois únicos estados tão premiados. Segundo o site do prêmio, Michigan “demonstrou resultados em todas as categorias da pesquisa, e líderes ágeis usam a modernização para implementar prioridades estratégicas e eficiência operacional. [Estes] estados mostram evidências de colaboração significativa; suas métricas e medidas de desempenho são amplamente adotadas; e os cortes no orçamento tendem a ser feitos de forma estratégica”.

Os esforços de treinamento de Michigan também foram selecionados pela NASCIO em 2013 como o principal projeto de segurança cibernética entre os 50 estados. Os detalhes deste prêmio podem ser encontrados no site www.nascio.org/awards.

O Sr. Ozols destacou que, de acordo com o documento do prêmio NASCIO, “várias ameaças cibernéticas graves foram evitadas diretamente com esses esforços” relacionados ao programa.

O Cyber Range tem sido amplamente aceito como uma arena avançada para treinamento de profissionais de segurança, e a Guarda Nacional usa o site para o seu próprio treinamento cibernético.

As medidas de segurança de dados de Michigan servem de modelo para outros estados. As equipes técnicas do Sr. Lohrmann explicou o impacto da Estratégia de resposta ao ataque cibernético na comunidade de segurança nacional, informando que ela foi considerada a melhor prática nacional pelo Departamento de Segurança Nacional. “Esta estrutura cibernética está sendo usada como exemplo do que estados devem fazer para coordenar com o setor privado em relação a infraestrutura crítica e segurança cibernética”, disse o Sr. Lohrmann.

Moradores e funcionários mais bem treinados e riscos à segurança reduzidos na mesma proporção são os benefícios mais importantes das iniciativas de treinamento de segurança cibernética de Michigan. As equipes técnicas do Sr. Ozols destacou que, de acordo com o documento do prêmio NASCIO, “várias ameaças cibernéticas graves foram evitadas diretamente com esses esforços” relacionados ao programa. Os danos decorrentes de tentativas de phishing e malware diminuíram e, considerando os custos elevados de graves brechas de segurança, os funcionários do estado de Michigan estimam o ROI do programa em “mais de 100-para-1”.

Além de programas de treinamento, as iniciativas também incluem segurança reforçada sob a forma de melhor infraestrutura de TI, como cabeamento, redes de dados, redes sem fio e projetos de computação móvel.

As iniciativas também forneceram um local de treinamento para indivíduos não residentes em Michigan e empregados que não são funcionários públicos. O site do estado contém informações atualizadas disponíveis para qualquer pessoa com acesso online. O programa Cyber Range oferece um local para treinamento estadual e nacional em medidas de segurança de dados. Além disso, as reuniões mensais do Sr. Lohrmann com executivos do setor e representantes da infraestrutura pública criam uma abordagem holística à segurança que vem sendo copiada a nível nacional.

Os programas também criam oportunidades de segurança e educação contínuas. A divulgação em escolas e a criação de iniciativas de segurança cibernética em colaboração com universidades de Michigan constituem um incentivo para os alunos buscarem as competências e o emprego nos campos de segurança de dados. Como observou o Sr. Lohrmann: “Postos de trabalho e desenvolvimento econômico podem ser o lado positivo da segurança cibernética”.

Lições aprendidas/Próximas etapas

As equipes técnicas do Sr. Lohrmann explicou que a obtenção de benefícios quantificáveis é sempre um desafio ao avaliar os benefícios dos programas de segurança. “No que diz respeito ao nosso treinamento, a parte mais difícil é não saber o que você desconhece”, disse ele. “Por exemplo: ‘Quantos ataques conseguimos interromper? Quantas pessoas não fizeram algo que não deveriam ter feito porque tinham o treinamento?’ É difícil.”

Ele continuou: “Calculamos o número de pessoas que vão receber o treinamento, analisamos suas reações a ele. Perguntamos se o comportamento delas mudou. Fazemos alguns testes para ver se as pessoas clicam em links, por exemplo. O problema em medir o nível de sucesso é que o fato de eu me sair muito bem na execução desses programas não significa necessariamente que vou influenciar o número de ataques contra nós. Não existe uma medida simples de segurança.”

“Acima de tudo, quando pensamos em dados, pensamos em como as pessoas interagem com eles, nos procedimentos que giram em torno desses dados e na tecnologia que utilizamos para protegê-los. Sob o ponto de vista da segurança cibernética, as pessoas são uma parte importante desse processo e é por isso que falamos tanto em treinamento.”

Dan Lohrmann,

Diretor de segurança (CSO), Diretor de segurança da informação (CISO) e Diretor-adjunto de segurança cibernética e proteção à infraestrutura do

Departamento de Tecnologia, Gestão e Orçamento de Michigan

As equipes técnicas do Sr. Lohrmann reconheceu que o ambiente de TI incentiva a coleta de grandes quantidades de dados. Ele aconselhou aqueles que pretendem criar programas similares a lembrarem que “nem todos os dados podem ser tratados da mesma maneira. Existem diferentes tipos de dados. Há dados confidenciais e não confidenciais. Saiba quais dados você tem. Descubra quais dados são importantes, como você os está protegendo e como pode compartilhá-los. Faça um inventário dos dados, saiba a que se referem, onde estão e qual é a finalidade deles. Há quanto tempo você os guarda? Há quanto tempo eles estão armazenados? Foi feito backup? Todos esses tipos de informações são essenciais”.

Identificar dados úteis e usá-los de forma adequada é o objetivo que o Sr. Lohrmann está tentando aprimorar. “Temos um projeto mais amplo que é compartilhar melhor os dados para obter resultados e revelar fraudes no governo ou descobrir programas para atender melhor às necessidades dos cidadãos, ligando os pontos que nos permitem fornecer melhores serviços aqueles que mais necessitam.”

As equipes técnicas do Sr. Lohrmann também descreveu a importância da criptografia de dados confidenciais, “tanto armazenados como em trânsito”. Ele disse: “Esta é uma política que demorou um tempo para implementarmos, mas já percorremos mais de 95% do caminho. Não chegamos aos 100%, mas estamos nos saindo muito melhor do que antes”.

As equipes técnicas do Sr. Lohrmann concluiu: “Acima de tudo, quando pensamos em dados, pensamos em como as pessoas interagem com eles, nos procedimentos que giram em torno desses dados e na tecnologia que utilizamos para protegê-los. Sob o ponto de vista de segurança cibernética, as pessoas são uma parte importante desse processo e é por isso que falamos tanto em treinamento. Não estou dizendo que somos perfeitos, mas temos que ter pessoas, processos e tecnologia em torno desses dados e precisamos ter certeza de que estamos refletindo sobre como estamos protegendo os dados dos cidadãos”.

Mais informações

Para obter mais informações, acesse http://www.michigan.gov/cybersecurity

Sede - América
Cisco Systems. Inc
San Jose. CA

Sede - Ásia e Pacífico
Cisco Systems (USA) Pad Ltd.
Cingapura

Sede - Europa
Cisco Systems International BV Amsterdam,
Países Baixos