STUART MADNICK, DO MIT: 'O HACKER TEM MAIS VANTAGENS NUM ATAQUE VIRTUAL'

Um dos maiores especialistas mundiais no combate a crimes virtuais, o professor do Massachusetts Institute of Technology diz que as empresas estão pouco preparadas para combater hackers

Leo Branco
08/06/2019 - 15:00

Stuart Madnick Foto: WS / WS

O professor americano Stuard Madnick, de 74 anos, é, provavelmente, o maior especialista do mundo nos efeitos de crimes virtuais sobre as empresas. Madnick pesquisa os percalços da tecnologia desde ingressar na prestigiada Massachusetts Institute of Technology (MIT), como aluno, em 1972. Cinco décadas depois, Madnick chefia um departamento da universidade – o MIT Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity (ou Consórcio Interdisciplinar para Melhorar a Segurança Cibernética da Infraestrutura Crítica) dedicado a estudar estratégias para as empresas criarem defesas contra hackers.

Entre os clientes estão negócios de porte como a bolsa de valores Nasdaq, as gigantes da tecnologia IBM e Phillips, e a mineradora Vale. Em cinco décadas, publicou mais de 380 livros e rodou meio mundo como professor convidado em universidades como Harvard, Nanyang (Cingapura), Newcastle (Reino Unido), Technion (Israel) e Victoria (Nova Zelândia) para abordar dos riscos virtuais inerentes às empresas. Para o especialista, como as empresas são idealizadas para darem certo, e serem funcionais aos seus clientes, pouco tempo das organizações é dedicado ao que pode não dar certo – como um ataque hacker bem-sucedido. Por isso, as mais do que investir em novos softwares antivírus, Madnick defende uma mudança no modelo mental das empresas.

Na entrevista a seguir, concedida durante visita a São Paulo em que palestrou na sede do recém-lançado banco digital C6, que vem utilizando o departamento de Madnick para construir sistemas resistentes a ataques virtuais desde o início, o especialista conta porque mudar culturas internas de uma organização mais difícil do que investir em sistemas.

O que faz o departamento faz no MIT?

O que a gente costuma fazer lá é se preocupar com pesquisas de novos hardwares ou softwares e firewalls, o que é tudo ótimo já que muitas empresas estão pesquisando esse assunto. A realidade é que 70-90% dos ciberataques são feitos por gente da própria empresa. Normalmente sem querer. Por exemplo, um funcionário que ao esquecer de sua senha a escreve num papel e deixa em algum lugar. Esse funcionário não é uma pessoa ruim, mas deu a uma pessoa má a oportunidade de acessar uma informação importante na sua empresa. O foco do

meu estudo é a estratégia de gestão das empresas para combater os crimes cibernéticos. Pouca gente presta atenção a eles, mas eles são o mais importante.

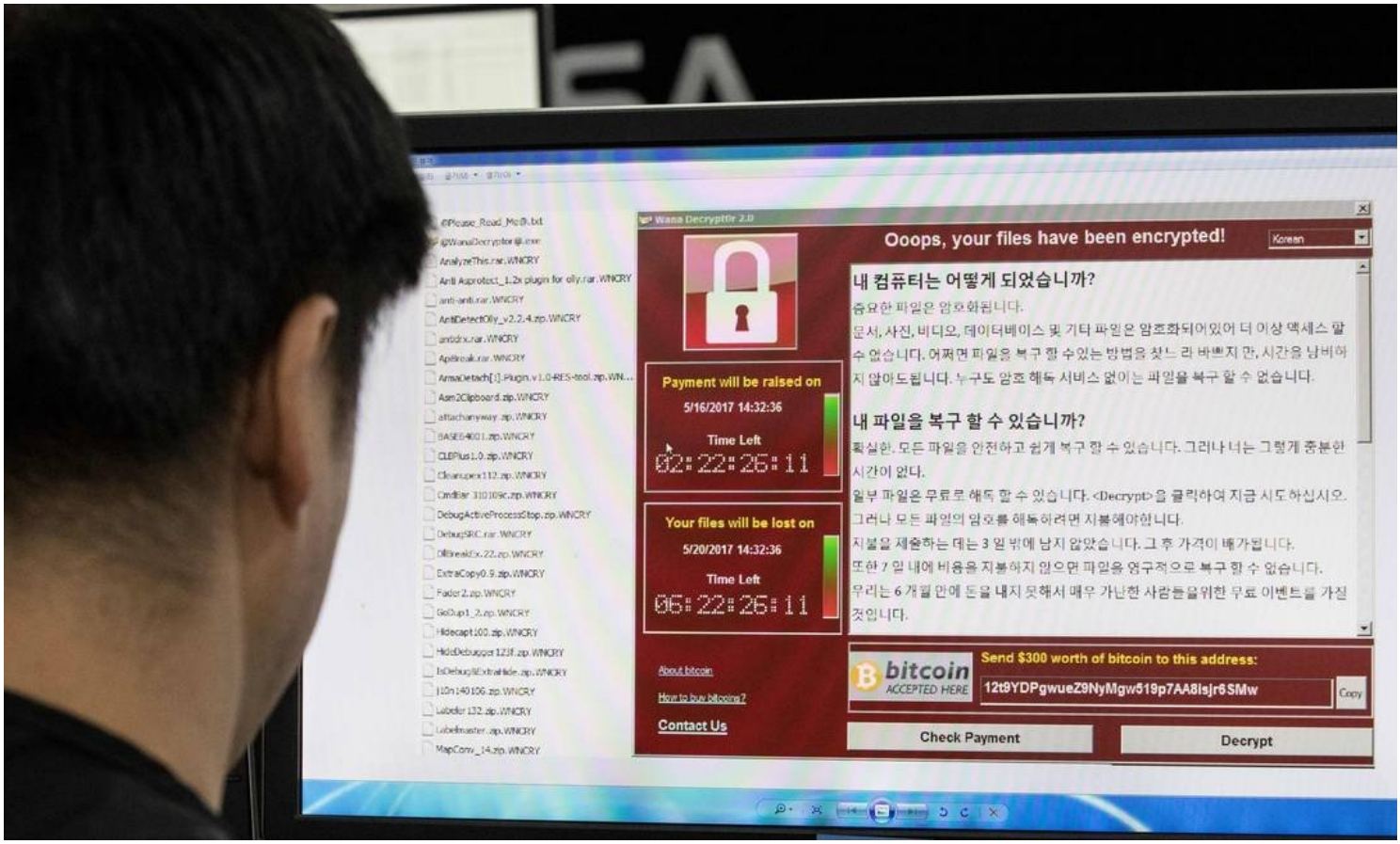
Por que as pessoas não prestam atenção a essas estratégias?

As pessoas comuns têm muitas concepções próprias quando o assunto é segurança virtual. Eu chamo essas concepções de mitos porque não estão corretas. Muita gente ao pensar num problema de segurança virtual lembra de dados do cartão de crédito sendo roubados. Nos Estados Unidos, você é responsável pelos primeiros 50 dólares gastos num cartão. Se eles foram gastos inadequadamente, o fato de alguém correr o risco de perder esse dinheiro faz com que as pessoas se preocupem em reportar eventuais roubos de dados. Mas isso não é o principal problema em segurança virtual.

Qual é a principal ameaça virtual atualmente?

São os que chamamos de ataques 'ransom', em que nada é roubado de você. O que acontece é que o software de um hacker entra no seu computador e trava o seu computador para que o verdadeiro dono dele não tenha acesso às informações lá dentro. Mais importante do que isso: pega os dados e os embaralha por completo. Nada é roubado, tudo está lá, mas não dá para fazer nada com o que está lá. Em 2017 um ataque desse tipo bloqueou 80% dos computadores da Telefonica (operadora de telefonia de capital espanhol). O que pode ser feito? Fechar uma companhia toda por um dia inteiro? Isso são eventos muito grandes, muito maiores do que uma pessoa ter um cartão de crédito roubado, mas ninguém fica sabendo,

infelizmente. Por quê? Porque as empresas atacadas não tem o menor interesse em demonstrar suas fragilidades.



Monitor exibe mensagem de bloqueio do vírus WannaCry na Agência de Internet e Segurança da Coreia do Sul (KISA) Foto: Yonhap / AFP

Mas os ataques ransom são um entre muitos casos de ataque que as empresas não querem falar a respeito. A primeira razão é a reputação delas. Não parece bom fechar a sua empresa por causa de uma fragilidade dessas. Além disso, encoraja outras pessoas a fazerem o mesmo ataque contra você. Se outro criminoso olha isso, pensa: "a Telefonica não é segura, vou atacar também". A ainda as consequências legais: um ataque virtual dá motivo para alguém pensar que os executivos de uma empresa não estão sabendo geri-la corretamente. Isso abre espaço para ações legais contra a companhia, que a farão perder mais alguns

milhões de dólares. Por muitas razões, as companhias estão sempre querendo evitar ao máximo a exposição desses casos de ataque. É por isso que, quando esses casos acabam ficando públicos, ainda assim as empresas negam terem sofrido esse tipo de ataque. E assim as pessoas comuns não sabem nada sobre esse tipo de ataque.

Por que as empresas são atacadas?

Essa é uma grande pergunta. Deixa eu fazer uma analogia: se você é o dono de um castelo, e precisa defendê-lo, você precisa garantir que todos os portões do castelo estarão fechados. Se você está no lado do hacker, só é preciso descobrir um portão que esteja aberto. É o que chamamos de uma guerra assimétrica. O hacker tem muito mais vantagens na luta contra o defensor de um sistema. Além disso, os softwares estão cada dia mais complexos -- estão muito próximos das complexidades dos humanos, para falar a verdade. Um software tipo tem centenas de milhões de linhas de código. É perfeitamente possível que uma dessas linhas não esteja bem escrita. Mas o problema não para aí. Há um problema de modelo mental. Quando uma pessoa está montando algo, seja um prédio ou um software, essa pessoa pensa em como essa estrutura deve ser utilizada para o bem e não todas as maneiras como essa estrutura pode ser mal-utilizada. Mas os hackers só pensam nisso: em como utilizar uma estrutura para o mal. As pessoas normais pensariam ao ver algo errado: "ok, isso não deveria estar acontecendo". Pois um hacker só funciona dessa maneira.

Colocamos dentro dos nossos softwares algumas pré-condições de uso desses mesmos sistemas sem pensar que um hacker vai usar esse software de maneiras que as pessoas normais nunca teriam pensado antes. E com consequências nunca

pensadas antes. Ninguém de maneira geral desenha um sistema, como um software por exemplo, com a intenção de vê-lo violado. Mas, na verdade, uma das razões pelas quais estou trabalhando com o banco C6 é que 15 ou 20 anos atrás quase ninguém sabia direito o que era cibersegurança. Eu venho falando disso desde 1979, quando escrevi um livro a respeito. Ou seja, não era algo invisível. Mas o que estamos vendo ao longo dos últimos 10 ou 20 anos é que as pessoas continuam desenhando softwares sem prestar a devida atenção a esses comportamentos "não usuais" por parte dos hackers.

Empresas precisam conferir segurança aos procedimentos e difuldir uma "cultura da ética" Foto: Pixabay

De onde surgem tantas vulnerabilidades?

Muito disso vem do fato de que a Microsoft, que desenhou a base da computação atual com o Windows, há 30 anos, também não pensou nessas vulnerabilidades. Ou, então, para ir a algo mais fundamental: a internet foi criada no fim dos anos 60

inicialmente para universidades colaborarem entre si. Dá para imaginar que uma universidade iria montar um ataque virtual contra você ou outra pessoa? Provavelmente não. Ou seja, as hipóteses sobre como a internet seria mal-utilizada não eram uma prioridade de quem criou a internet lá atrás. Quem criou a internet vivia num mundo universitário americano, naquelas comunidades em que é possível deixar a porta de casa aberta e ninguém vai roubar suas coisas. Havia confiança um nos outros. Ninguém imaginava que a internet poderia ser utilizada para fazer o mal ou para quebrar a confiança de alguém.

A lógica de segurança virtual que muitas empresas estão pensando hoje em dia, e o C6 está pensando já desde o momento de criação dos sistemas, aconteceu relativamente tarde nas empresas de maneira geral. E aí o resultado é que elas estão precisando analisar milhões de linhas de código 20 ou 30 anos depois de eles terem sido desenhados. É uma ação que demanda um esforço tremendo nas empresas. Queremos desenhar com o C6 um sistema protegido a ataques de hackers já desde o início.

Como desenhar sistemas totalmente imunes a ataques -- ou pelo menos muito perto disso?

Há cada mais aparelhos conectados à internet dentro do conceito de internet das coisas. Minha mulher, por exemplo, já tem uma escova de dentes inteligente. Ela pode ser conectada à internet e informar ao dentista se ela está escovando corretamente ou não. Pois bem, duvido que quem criou a escova de dentes inteligente pensou em como essa escova pode ser atacada por um hacker. Provavelmente nem passou isso pela cabeça de quem criou. Outro exemplo são as

geladeiras inteligentes. Elas saem de fábrica com câmeras internas para avisar ao dono, através de um aplicativo de celular, os produtos em falta em casa.

Tudo isso é processado por computadores embarcados dentro da geladeira. Pois bem, já vi casos de geladeiras inteligentes hackeadas em que o computador, que deveria estar gerenciando o nível de gelo ou a temperatura do freezer, estar, na verdade, encaminhando mensagens pornográficas na internet. Então, além de pensar em como elas estão fazendo gelo ou mantendo a temperatura correta, o designer da geladeira inteligente precisa pensar: como proteger o aparelho de um ataque hacker? O problema é que nosso modelo mental não está preparado para usos bizarros das estruturas que criamos.

Ataque hacker Foto: Kacper Pempel / Reuters

É possível rastrear as vulnerabilidades?

Acredito firmemente que as empresas já estão desenhando sistemas mais seguros. Faço a analogia com a construção civil. Vamos lembrar que a construção do Empire State Building, um dos maiores prédios do mundo, nos anos 20, morreram 120 operários. As pessoas não achavam que a segurança no trabalho era algo importante. Isso foi há 90 anos. De lá para cá, por pressão da sociedade e da opinião pública, as empresas passaram a se preocupar com a segurança num canteiro de obras. Isso resultou em mudanças positivas ao longo desses anos. É muito comum ver placas em canteiros de obras hoje mundo afora com os dizeres: "estamos a 100 e poucos dias sem acidentes e por favor não seja a pessoa que vai fazer voltar esse contador para zero". As pessoas são forçadas a fazer um bom serviço e a trabalhar com segurança. Demorou algum tempo para acontecer em linhas de produção do mundo real. E é esse tipo de adaptação de modelo mental que estamos tentando incutir nas empresas no que diz respeito à proteção delas sobre cibersegurança.

De que maneira é possível mudar esse modelo mental?

O que tentamos é entender é quais poderiam ser as melhores técnicas ainda não inventadas para prevenir problemas em estruturas físicas? E, num segundo momento, queremos entender: como adaptar essa mesma lógica aos ataques virtuais? Ou seja, como fazer nossas redes virtuais seguras da mesma maneira que tornamos nossas fábricas mais seguras? Estamos aplicando uma técnica desenvolvida por um de nossos pesquisadores no MIT do departamento de aeronáutica. Ele passou 20 anos pesquisando formas de reduzir acidentes aéreos. Estamos adaptando as técnicas dele para segurança virtual. Esse método envolve dois passos chave.

O primeiro é relativamente simples, mas pouco lembrado: tem clareza do que é importante em sua empresa. Você pode perguntar ao seu chefe: qual é a coisa mais importante na sua organização. Aposto que ele vai dizer centenas de coisas. Poucas pessoas se preocupam em entender aquilo que de fato é realmente importante. A maioria dos executivos nunca pensou muito bem nisso. Se você não consegue focar no que de fato é importante você não consegue se proteger de verdade. Parece simples mas é extremamente difícil para a maioria dos executivos, muitos deles treinados a pensar de outra maneira.

Isso é relativamente óbvio para a indústria da aviação: a prioridade máxima é o avião não cair. A televisão de bordo não funcionar, bem, isso certamente é chato mas a prioridade é o avião não cair. Ter esse foco é importante sobre o que precisa ser protegido. A segunda parte é onde a engenharia de fato começa. Tudo o que acontece dentro de uma empresa faz parte de um processo interno. Fazer uma entrevista, por exemplo, é um processo. Cada processo, em geral, tem algum tipo de monitoramento ou controle. O seu chefe ao ver o resultado da entrevista pode pensar: ele fez um bom trabalho? Se não, que tipo de treinamento ele precisa ter para fazer um bom trabalho? Mas aí o seu chefe também sofre algum tipo de controle. Em muitas empresas há hierarquias com muitos níveis de controle. E isso é um problema.

Por quê?

É muito comum haver problemas no desenho dos controles desses processos. Muitos das vulnerabilidades de sistemas detectadas por quem está na base acabam

nem chegando ao nível da alta gestão, que tem poder para tomar as decisões corretas para aumentar a segurança de um sistema. O motivo: as pessoas não conversam entre si dentro de uma empresa.

A SEGURANÇA QUE GARANTE O SIGILO DAS REDES DE DESINFORMAÇÃO NO WHATSAPP

POR QUE EU ESTOU PREOCUPADO COM O GOOGLE

COMO O GRUPO MULHERES CONTRA BOLSONARO FOI HACKEADO NO FACEBOOK

COMO FUNCIONA O MAIOR GRUPO DE PROPAGAÇÃO DE ÓDIO NA INTERNET BRASILEIRA, QUE LUCRA COM MISOGINIA, RACISMO E HOMOFOBIA

As grandes empresas de tecnologia como Google, Facebook e Amazon já nasceram num mundo digital e têm estruturas de gestão consideradas modernas. Elas também sofrem com esses problemas?

Sim porque elas surgiram há 15 ou 20 anos e, embora tenham feito mudanças para aperfeiçoar seus sistemas, são empresas que cresceram muito e muito rápido. Além disso, foram criadas sob a lógica de um mundo amigável e em que essa enorme quantidade de ataques virtuais não existiam. Mas tem uma coisa mais perigosa por trás da expansão de redes sociais e de sites que coletam nossos dados.

Por causa do compartilhamento dessas informações, hoje está relativamente fácil criar golpes virtuais com pedidos de dinheiro. Se, no passado, eram comuns aqueles e-mails fantasiosos como "um príncipe da Nigéria gostaria de lhe mandar um dinheiro mas para isso precisa do seu cartão de crédito", hoje em dia é possível um golpista montar um e-mail bastante verossímil apenas rastreando todo tipo de informação que as pessoas postam online. A inteligência artificial hoje já permite rastrear todas essas informações de modo a permitir e-mails de golpes bastante personalizados. Cerca de 70% dos ataques desse tipo são bem-sucedidos.

E o que as pessoas devem fazer? Desligar suas redes sociais?

Bem, na idade das cavernas, ninguém sofria com ataques virtuais, mas não imagino que as pessoas queiram voltar àquela realidade só para livrarem-se dos perigos online. É um desafio grande porque tudo na vida é um risco. Levantar da cama é um risco: você pode escorregar no chão do quarto, ser atropelado por um carro ao sair de casa e por aí vai. Tem que julgar: é claro que a vida digital traz riscos mas é preciso julgar os benefícios possíveis com a tecnologia. A lógica aqui tem que ser: como maximizar benefícios e reduzir riscos?

Mas, dentro de uma empresa, como fazer isso?

A grande maioria das falhas de segurança numa empresa acontecem nas interconexões entre departamentos. Ou seja, você sabe o seu trabalho, mas o editor de outra área não sabe o que você faz. Ele está focado no trabalho dele. Poucas pessoas nas empresas conseguem fazer a relação sobre como os dois trabalhos estão correlacionados. Além disso, há o risco de exposição de dados a um terceiro

externo à organização. O veículo de comunicação que você trabalha pode ter a melhor segurança virtual do mundo. Mas a gráfica que imprime o jornal ou a revista pode não ter. Essas suas estruturas estão conectadas. O hacker pode vir através da gráfica e atacar a redação. Isso não é algo que as empresas costumam prestar atenção e também requer uma mudança grande de cultura.

Mas, voltando ao início da conversa: quantas pessoas morrem hoje em dia na maioria dos países desenvolvidos na construção de edifícios? Poucos ou quase nada, uma grande mudança em relação ao que morriam na época da construção do Empire State Building. Se você consegue mudar a maneira como pensa e age em relação a um determinado problema, a transição pode mais fácil. A mesma mudança pode levar dez ou mais anos para ocorrer na segurança virtual. De todo modo, ela poderá nos permitir construir sistemas muito mais seguros que os existentes atualmente.

ANTERIOR

ERNESTO ARAÚJO RESPONDE A MOURÃO, QUE ELOGIOU VICE-CHANCELER

PRÓXIMA

BOLSONARO E A ÉGIDE DO EXCESSO [ARTIGO]