CISION

Exame

ID: 75240825

01-06-2018

Meio: Imprensa
País: Portugal
Period.: Mensal
Âmbito: Economia, Negócios e.

Pág: 28
Cores: Cor
Área: 18,60 x 24,30 cm²
Corte: 1 de 5

EXAME

Micro

EMPRESAS . NEGÓCIOS . GESTÃO

TECNOLOGIA

Eles andam de olho na sua empresa

Já ouviu falar em Bug Bounty? Sabe como funciona um hacker? Altere comportamentos e teste a segurança da rede informática da sua empresa para evitar prejuízos futuros

Texto ***Cesaltina Pinto***

Sara tem 43 anos, é divorciada e está a trabalhar no departamento de marketing da empresa do pai, na indústria de confeções. Sara costuma acompanhar o pai às feiras internacionais. Atende clientes, é relações públicas, distribui cartões, recolhe contactos. Entre as suas funções, está também a gestão das páginas da empresa nas redes sociais, nas quais vai partilhando fotos e outras informações. Entre essas páginas e o seu perfil pessoal no Facebook e Instagram, Sara vai mostrando o que vende, com quem fala, o que come, o que veste, do que gosta, com o quê e com quem se entusiasmou.

Um dos contactos profissionais que fez até lhe pediu, depois, amizade no Facebook. Sara aceitou. É descomprometida, bonita, sociável, está aberta a outros possíveis compromissos. Uns meses depois, essa "nova amizade" desapareceu sem deixar rasto. Foi pena, até porque ela queria dizer-lhe que já tinha comprado os tais sapatos por ele recomendados no link que lhe enviou.

"O objetivo é sacar dinheiro ou dados, que têm muito valor no mercado negro cibernético"

Sara estranhou, mas não pensou mais no assunto. E entretanto andou num sufoco. Alguém entrou no sistema informático da empresa e apoderou-se do email do pai, o presidente do Conselho de Administração. Este só percebeu que algo estava errado, quando começou a estranhar o atraso no pagamento de contentores de mercadoria enviada. E quando contactou os destinatários recebe de volta a resposta de que os pagamentos tinham sido fei-

CISION
Exame
ID: 75240825
01-06-2018
Meio: Imprensa
País: Portugal
Period.: Mensal
Âmbito: Economia, Negócios e.
Pág: 29
Cores: Cor
Área: 18,60 x 24,30 cm²
Corte: 2 de 5

tos para outra conta, tal como ele tinha pedido. A verdade é que ele nunca tinha pedido isso, mas a outra parte apresentou o email (supostamente) enviado por ele. Ficou branco como cal, pois o email era efetivamente o dele, tal qual. Reviu todas as situações e percebeu que a fraude era já de alguns milhares de euros. E agora?

A empresa socorreu-se de advogados e de serviços de cibersegurança, mas, entretanto, perdeu acesso a dados de clientes. Estavam encriptados ou cifrados. Para tê-los de volta teria de proceder a alguns pagamentos. Caso contrário, acederiam a seguir diretamente às suas contas bancárias. Os homens da cibersegurança traçaram o mapa da mina, viram todos os cantos à casa e perceberam que o rei estava nu, ou seja que o castelo estava desprotegido, sem sentinelas adequadas, sem muralhas e com os portões da tecnologia abertos. E seguir a pegada digital do criminoso seria mais difícil do que procurar uma agulha num palheiro. A coisa foi de tal ordem que, no final, à empresa só restou fazer implodir o castelo e declarar falência. Bem-vindo ao mundo do cibercrime.

A Sara não existe, mas de certeza que muitas pessoas se reviram nela. A situação descrita configura a tipicidade de um cibercrime dos dias de hoje, em que a indústria exportadora, como os têxteis ou o calçado, é um alvo fácil para hackers mal-intencionados. Apertados pela crise dos últimos anos, os industriais de pequena e média dimensão apostaram na tecnologia sobretudo para produzir, exportar e agilizar funcionalidades. A segurança dos seus sistemas ficou sempre para segundo plano. Agora, o prejuízo pode ser bem maior do que o investimento que teria sido necessário. E basta a entrega de um cartão numa feira ou um clique distraído, e aparentemente inofensivo, para pôr em risco todo o modelo de negócio.

FRAQUEZA DAS MULHERES: AS REDES SOCIAIS

Bruno Castro, 42 anos, engenheiro eletrotécnico e um dos três sócios-fundadores da VisionWare, empresa de segurança de computadores, anda nisto há 13 anos. Melhor: há mais, porque muito antes de fazer das suas competências um negócio, também ele andou no *dark side*, como *hacktivista*. Como gosta de furar sistemas desde miúdo, sabe muito bem como se faz. Agora, usa os seus conhecimentos para testar a segurança das empresas e reforçar os seus portões eletrónicos. Gere um grupo com cerca de 60 investigadores que trabalham para todo o mundo, não só em grandes empresas como noutras mais pequenas (o centro de operações logísticas em Cabo Verde serve de ponte aérea para África), mas também tem a Comissão Europeia e a NATO no seu cardápio. Chegou atrasado ao encontro com a EXAME porque andava a tratar de cinco ataques informáticos simultâneos, com características similares ao anteriormente descrito.

É ele que nos transporta para a forma de pensar de um hacker que opta pelo crime. Na maior parte das vezes, o objetivo é sacar dinheiro ou dados, os quais também são uma fonte de rendimento e têm muito valor no mercado negro cibernético. E como se faz?

"As mulheres são um problema. O que publicam nas redes sociais dá um jeitão. O que elas tornam público é utilizado pelo criminoso para benefício próprio: os seus gostos pessoais, com quem fala, por onde anda, com quem interage, se tem 50 anos, se é divorciada, se está com vontade de conhecer mais pessoas... Se eu criar um perfil falso, seduzo-a e socialmente ganho a sua confiança... vamos andando, tenho esse tempo até conseguir cativá-la. É uma pesca à linha, demora meses, mas tenho tempo", simula Bruno Castro. "Chama-se isto estudar o alvo."

"A partir daí percebo se é uma pessoa importante dentro da empresa, se é filha do dono, se é financeira... Se é homossexual e, se está metida em grupos mais restritos, também me envolvo. Se não conseguir cativá-la dessa forma, penso noutro tipo de ataques: saber se compra sempre online, sapatos ou roupa... Envio emails contínuos de tudo quanto é sapatos, roupa... e sempre que aparecem as imagens, também aparecem os pop-ups. O que ela vai fazer? Clicar naquilo para ver as fotos. De cada vez que está a clicar ou está a dar permissões para usar os seus dados pessoais para fins comerciais, pode estar a *infetar-se*."

Se o processo de estudo é longo, o ataque

NÃO DEIXE PARA AMANHÃ O QUE PODE FAZER HOJE

Na era da internet, todos os cuidados são poucos. Aqui ficam alguns conselhos a ter em conta

> AVALIE O RISCO

Faça uma análise do potencial prejuízo em relação ao investimento, veja o que pode correr mal e se é apetecível como alvo (valor dos dados, uso de criptomoeda, valores exportados, o contexto dos países com que negoceia, etc.). Se os potenciais prejuízos forem superiores ao custo, então não há que hesitar: reforce a segurança do sistema.

> CONHEÇA A SUA EMPRESA

Audite, valide, faça análises clínicas regulares, stresse a infraestrutura. Teste, teste, teste. Não espere que aconteça algo que será difícil remediar. Resolva dois problemas agora, para depois não ter de resolver 40 de uma só vez.

> MODELO DE GOVERNANCE

Defina regras e várias formas de validação. Encare a segurança de forma integrada. As normas internacionais de boas práticas para a segurança da ISO 27001 podem ser um bom começo.

> MUDE A MENTALIDADE

É preciso outro modo de fazer as coisas e tudo, agora, tem de ser permanentemente readaptado. O cibercrime está apenas no início. Por isso, se um hacker lhe reportar um erro, sem o chantagear, agradeça-lhe e recompense-o. Foi a sua empresa que ficou a ganhar com a identificação de um erro que acabaria por lhe trazer prejuízos.

GETTY IMAGE

CISION
Exame
ID: 75240825
01-06-2018
Meio: Imprensa
País: Portugal
Period.: Mensal
Âmbito: Economia, Negócios e.
Pág: 30
Cores: Cor
Área: 18,60 x 24,30 cm²
Corte: 3 de 5

ANDRÉ BAPTISTA / Most Valuable Hacker

"O DESAFIO É ANDAR MAIS RÁPIDO DO QUE A SEGURANÇA"

Com 24 anos, este "hacker-versão-boa" destacou-se, em Washington, como o mais valioso do mundo, pela criatividade com que conseguiu furar a segurança da plataforma norte-americana Mapbox

FERNANDO VELUDO/NFACTOS

Quando começou a fazer isto?
Explorei sozinho a informática e descobri um livro de programação que o meu pai tinha. Li-o e comecei a perceber como os computadores funcionavam. Devia ter uns 11 anos. Comecei a fazer uns sites... Fiz um para a disciplina de Área de Projeto, teria 14 anos. No 9º ano, já sabia programar um bocadinho. Pensei em ir para um curso profissional de informática, mas depois seria difícil entrar na universidade por causa da Matemática. Então, no secundário, fui para Ciências e Tecnologias. Tive, então, todas as bases da Matemática e logo aí comecei a explorar a segurança. Sempre achei engraçado ver, nos filmes, a entrarem num computador e interrogava-me se era possível.

Gostava de fazer o que não devia?
Um bocadinho [*risos*]. Depois ganhei consciência do que não podia fazer. Nunca entrei ilegalmente num site, OK? Mas preguei muitas partidas, ao ponto de o meu pai ter sido chamado à escola. Uma vez, a professora ia apresentar um PowerPoint e eu fiz um código para pôr o compartimento dos CD sempre a abrir e a fechar. Durante toda a aula ouvimos o abrir e o fechar do CD. Os colegas adoraram, a professora nem por isso. Confessei a culpa. A professora, furiosa, ameaçou processar-me. Tinha 15 ou 16 anos, a idade de fazer asneiras. O próprio informático da escola não acreditava que eu tinha conseguido fazer isso. Só quando removi o código é que ele acreditou. Punha também os telemóveis dos colegas a mandar mensagens de uns para os outros. Depois licenciei-me em Informática, em Coimbra. Vim para o Porto, em 2015, fazer o mestrado em Segurança. Fiquei logo à frente da equipa dos CTF [Capture the Flag], onde tenho aprendido muito.

O desafio é furar os sistemas?
Sim. E tentar andar mais rápido do que a segurança evolui.

Há em si um fora-da-lei?
Tem de haver a consciência do que podemos ou não fazer de forma legal. Se somos boas pessoas, não prejudicamos ninguém nem nenhuma empresa. É uma área muito divertida. E quando conseguimos resolver um desafio, isso é muito gratificante e até conseguimos ganhar bastante dinheiro.

Qual foi o seu maior desafio?
Os concursos da HackerOne. Na primeira vez que concorri, em Las Vegas, no ano passado, não descobri nada, foram três dias e três empresas. Pensei que nunca mais me voltariam a sinalizar. Mas qualifiquei-me depois num CTF, em Washington, com um segundo lugar. Deram-me uma nova oportunidade. Andei dois meses a estudar e a explorar muita coisa. Os CTF são complexos, mas simulados, é algo completamente diferente de uma situação real. Aprendemos as técnicas, mas na realidade do Bug Bounty temos de saber onde procurar numa grande superfície de sites e serviços. Desta vez esforcei-me e encontrei vários erros, entre os quais uma falha crítica. Devido ao esforço, e criatividade, atribuíram-me o título de *most valuable hacker*, o vencedor. Foi uma honra trazer o título para cá. Mostrou que Portugal tem pessoas boas nesta área e que já não é só o País que ficou à sombra da bananeira desde os Descobrimentos, como disse o CEO da HackerOne. Vamos começar a dar cartas na cibersegurança.

"A segurança é crucial para o negócio. Quem tem estes conhecimentos devia ser mais bem pago"

CISION
Exame
ID: 75240825
01-06-2018
Meio: Imprensa
País: Portugal
Period.: Mensal
Âmbito: Economia, Negócios e.
Pág: 31
Cores: Cor
Área: 18,60 x 24,30 cm²
Corte: 4 de 5

Conseguiu que a empresa lhe mandasse um token?
Valeu-me 7 500 dólares. Encontrei uma vulnerabilidade num processamento e fiz com que o servidor enviasse um código de acesso ao sistema administrativo. Agora, já não preciso de qualificar-me, passei a ser convidado.

Diz-se que o verdadeiro hacker não mostra o rosto?
Esse é o preconceito e o estereótipo. Não diria que é o verdadeiro, mas que é o hacker mau. Para mim, ser hacker é um *mindset*, é conseguir contornar proteções, ser criativo, resolver desafios, ultrapassar problemas, arranjar forma de dar a volta. Um bom hacker é aquele que consegue usar estes conhecimentos de forma inteligente e para o bem da Humanidade. Tem de ser uma boa pessoa.

Onde está o génio: no que cria ou no que descobre as falhas?
É complicado. Quem cria pode ser muito bom, mas quem descobre falhas tem também de perceber como o sistema foi concebido e onde houve desleixo. Às vezes são coisas lógicas que escapam a quem as cria. Os programadores ainda não têm salários muito atrativos em Portugal e vão para fora ganhar cinco ou seis vezes mais. Quem fica muitas vezes tirou um curso sem as bases da segurança e acaba por cometer erros a desenvolver soluções. A segurança está em explosão e deveria ser a prioridade – é crucial para o negócio. E quem tem estes conhecimentos deveria ser mais bem pago.

Há gente a espiar o nosso telemóvel e computadores? Devemos mesmo tapar as câmaras?
No meu computador tenho sempre uma fita a tapar a câmara. Num telemóvel é mais complicado. Mas é possível espiar através da câmara, sem que a luz acenda e a pessoa saiba que a câmara está ativa. As pessoas devem prevenir-se.

tem de ser silencioso para não ser detetado, e rápido para roubar o máximo no menor tempo possível. "Isto é um jogo", prossegue Bruno que insiste: "É preciso explicar: o elo mais fraco são as pessoas, não propriamente a tecnologia. Quando faço um ataque de phishing e ela clica no link, é um ataque à pessoa, não à tecnologia. Se carrega no link, já está apanhada. A partir daí já estou lá dentro, a máquina já me pertence, e eu começo a disseminar-me: roubo os seus dados pessoais, uso a identidade dela e a pessoa até trabalha numa empresa que me interessa... Com um ataque de speed phishing, conseguimos infetar o seu computador pessoal ao ponto de vermos a câmara e tudo o que ela escreve no teclado em tempo real, visitar os sites dela, o homebanking. Às vezes esse vírus nem sequer é detetado pelo antivírus."

Para Bruno Castro, tem sido "muito difícil" explicar à "geração dos 40, 50 ou 60 anos", ou "dos 14 aos 17", que tem de aplicar nas redes sociais os mesmos sistemas de autodefesa aplicados na rua. Quando pensa que navegar na internet no conforto do sofá lá de casa lhe dá segurança, pense que o criminoso pode também estar a assaltar a sua conta bancária, ou a da sua empresa, igualmente sentado no sofá e a milhas de distância.

Edgar Pimenta, 44 anos, chefe de segurança da Talkdesk, confirma: "O cibercrime já não é como nos anos 80: um jovem que anda lá em casa a fazer umas brincadeiras. É uma estrutura organizada e sofisticada, com vários níveis, que anda sempre um bocadinho mais à frente. Muitos têm recursos para estar a atacar as empresas 24 horas, continuamente."

Os ataques podem ser em massa, por ondas. Varrem tudo, independentemente do alvo principal. E têm sido cada vez mais exponenciais. Ainda está fresca a memória do último ataque cibernético que lançou o ransomware WannaCry e deixou o governo inglês com as mãos na cabeça. Foi em massa, transcontinental e atacou instituições públicas e privadas em várias partes do mundo. "Usou a forma de ataque por phishing, em que se recebe um email falso, clica-se nele e é-se *infetado*, aproveitando uma vulnerabilidade do sistema da Microsoft para se espalhar na rede. O que faz: infeta, puxa tudo do computador para a internet, encripta e depois pede um resgate. É um ataque de delito comum nas empresas, encriptar a base de dados do negócio e exigir um pagamento para desencriptar a informação. É ótimo para se ganhar dinheiro. Peço €1 000 ou €5 000 a quem for apanhado. Se ganho dez por cento de milhares e milhares, façam as contas...", adverte Bruno Castro.

"O cibercrime anda sempre à frente, tem vários níveis e recursos para atacar continuamente"

A maioria paga, pois não são valores altos, já que não quer ficar sem aceder aos seus sistemas durante dias. Aliás, grande parte nem quer que se saiba. E quando se recupera o sistema, a prioridade não é apanhar o infrator, mas perceber se ele ainda está lá dentro e reforçar a segurança.

BUG BOUNTY, PRECISA-SE

E como anda a segurança das nossas empresas, sobretudo quando muitas delas também já criaram os seus sistemas de venda online? Nos últimos anos, alguma coisa tem melhorado. Edgar Pimenta considera que "muitas não estão preparadas", nem o estarão enquanto a segurança não for encarada como fundamental e estiver embebida nos procedimentos da empresa. "Para muitas, isto ainda nem sequer é um tema. E não é uma tarefa fácil, porque é uma questão de mentalidades", diz o chefe da segurança da Talkdesk que gere clouds de outras empresas.

Bruno Castro, que estima que a VisionWare vai faturar neste ano três milhões de euros, admite que a segurança melhorou nos últimos cinco anos, é cada vez mais uma preocupação e os sistemas são mais resilientes. "O problema é quando se leva o computador para casa e o expõe à selva, aos perigos do mundo cibernauta. Se o computador regressa infetado, e se não houver mecanismos tecnológicos e procedimentos internos, depois dissemina o ataque na rede."

CISION
ID: 75240825
Exame
01-06-2018
Meio: Imprensa
País: Portugal
Period.: Mensal
Âmbito: Economia, Negócios e.
Pág: 32
Cores: Cor
Área: 18,60 x 24,30 cm²
Corte: 5 de 5

Edgar Pimenta, da Talkdesk
O responsável de segurança lembra a grande evolução no cibercrime nos últimos anos


LUCÍLIA MONTEIRO


LUCÍLIA MONTEIRO

Bruno Castro, VisionWare
Há 13 anos que usa as suas competências de hacker para testar a segurança informática

Ambos sabem que "há ainda muito a fazer", até porque a segurança dos sistemas informáticos é um processo contínuo, sem garantia total. Por isso, é preciso "testar, testar, testar...", um conceito ainda pouco compreendido pelos nossos empresários. Que o diga André Baptista, investigador do Centro de Sistemas de Computação Avançada do INESC TEC e mestre em Segurança Informática pela Faculdade de Ciências da Universidade do Porto (FCUP). Com 24 anos, gere uma equipa de hackers "bem-intencionados", na universidade, que testa sistemas em ambiente simulado e encontram sempre forma de entrar. Foi assim que André se qualificou para ir ao encontro da plataforma HackerOne, na qual empresas de todo o mundo desafiam os melhores hackers a entrarem nos seus sistemas. Se encontrarem falhas, elas são reportadas, a segurança reforçada e os hackers devidamente recompensados – daí o nome Bug Bounty. André Baptista assim fez e ganhou o título de melhor hacker do mundo numa das competições em Washington, realizada em finais de março.

O que ele gostava era de ver empresas portuguesas num programa destes, ou até mesmo de criar um por cá. "Tenho um exemplo de um investigador português que descobriu uma falha numa empresa, reportou-a e não pediu dinheiro. Os representantes da empresa mandaram uma carta de um advogado a exigir que ele corrigisse o problema, quando ele nem sequer era o responsável. Quem tinha programado é que tinha lá deixado o erro. Reportou a falha de forma ética, para que a empresa ficasse mais segura, e foi ameaçado por um advogado, porque ele nem devia ter-se atrevido a entrar ali. Isto é tudo o que não se deve fazer. Se uma empresa não tiver um programa de Bug Bounty é muito complicado descobrir as suas vulnerabilidades", conta.

Face à falta de profissionais nesta área, o melhor é cativar quem está do lado negro do sistema e trazê-lo para o lado certo. "Se alguém reporta uma vulnerabilidade de boa-fé, a empresa devia agradecer. Se não puder pagar, até pode fazer um reconhecimento público, pois contribui para o currículo. Se pagar, melhor. É bom para as empresas que evitam prejuízos futuros e a fuga de dados. E quem for mal-intencionado perceberá que não vale a pena correr riscos a vender dados ou a prejudicar empresas."

"Se a empresa não tiver um programa de Bug Bounty não descobre as suas vulnerabilidades"

Não é por acaso que as grandes empresas como o Facebook, Google ou Twitter têm os seus próprios programas de Bug Bounty. E mesmo assim... Lembre-se de que o vírus anda sempre à frente do antibiótico.