Criminosos cibernéticos: a grande ameaça

MARÍA ÁNGELES CABALLERO VELASCO
Direcção de Apoio Geral de Segurança e Meio Ambiente MAPFRE

A tecnologia tem avançado a passos gigantescos desde que nasceram os primeiros computadores pessoais na década de 1980, como o *Spectrum,* até os mais sofisticados sistemas de que podemos dispor hoje, desde dispositivos móveis que nos permitem estar conectados em qualquer lugar do mundo até a "Internet das Coisas", objetos do cotidiano interligados uns aos outros our por meio de uma rede. A proliferação das redes sociais, o aumento do consumo de serviços web e a revolução da nuvem ou *cloud* deram ainda mais força à nova era de dispositivos interconectados.

Este novo cenário tem feito com que usuários, empresas e governos mudem seu comportamento, sua forma de interagir com o meio. Hoje as empresas são totalmente dependentes das tecnologias da informação (TI). É inconcebível que uma empresa não tenha o respaldo da tecnologia para funcionar corretamente, e por isso os equipamentos de TI e sua segurança são peças-chave nas organizações. Imagine uma catástrofe cibernética que pudesse afetar vários setores e inúmeras companhias no estilo do "Duro de Matar 4.0"? Isto causaria a interrupção de suas atividades e o roubo ou dano de seus sistemas de computação, o que em alguns casos poderia ter efeitos diretos ao estado de bem-estar de um país (usinas nucleares, empresas de energia, etc.). Estimou-se que, se a atividade das empresas forem paralizadas durante uma semana, o impacto econômico poderia chegar a 10 bilhões de dólares[1].

O auge da tecnologia que estamos vivendo nas últimas décadas traz consigo um aumento do risco tecnológico, em especial nos últimos anos, principalmente porque isso colocou à disposição dos criminosos cibernéticos um novo mundo de fraudes com a consequente criação de novas formas de realizar crimes por meio da tecnologia. Esta situação tem causado uma preocupação crescente nas empresas, o que as tem levado a criar equipes especializadas dedicadas exclusivamente ao controle e à supervisão destes riscos (as chamadas *blue teams),* chegando, inclusive, à resposta para possíveis incidentes de segurança.

Para que se possa entender esta situação, desenvolveremos brevemente o conceito do **risco** de uma perspectiva empresarial, medido como o produto das **ameaças**, vulnerabilidades e seu impacto sobre o negócio. Podemos compreender o risco como cenários possíveis que podem comprometer total ou parcialmente os recursos de uma empresa, colocando sua viabilidade em perigo. Consequentemente, para contrabalançar este risco, as empresas devem estabelecer as medidas adequadas para mitigar, evitar, transferir ou aceitar estes riscos. Exporemos quais ameaças estão à nossa espreita na Internet e depois, as **contramedidas** para atenuar e gerenciar essas ameaças.

AMEAÇAS CIBERNÉTICAS, FRAUDE E CRIMES NA REDE

Os "maus" todo ano reinventam novas formas de realizar crimes telemáticos, mas também é verdade que existem algumas ocorrências que vêm se repetindo ao longo dos anos, e algumas delas vêm diminuindo. O *spam*, por exemplo, caiu 50% em uma década, de acordo com o último *Intelligence Report* da Symantec.

Os ataques mais populares têm como objetivo tanto servidores de empresas quanto dispositivos de usuário final. Os ataques físicos estão começando a ser menos comuns, mas os ataques sociais vêm aumentando nos últimos anos. As **principais ameaças cibernéticas**[2] que as empresas enfrentaram no passado ano podem ser descritas por meio de nove padrões: ataques a websites (35%), espionagem cibernética (22%), intrusão em pontos de venda ao cliente (14%), cópia ilegal de cartões de crédito (9%), uso indevido de sistemas por funcionários internos (8%), software mal-intencionado ou *malware* (4%), erros diversos (2%), roubo ou perda física (< 1%) e ataques de recusa de serviço (<1%). Para este ano de 2015 já se calcula que as perdas econômicas que as empresas europeias sofrerão ultrapassarão 14 bilhões[3] de euros devido a ataques cibernéticos, e estes ataques não são apenas econômicos, mas também reputacionais. Cabe destacar que a Espanha é o terceiro país com mais ataques cibernéticos do mundo, depois dos Estados Unidos e do Reino Unido.Vejamos como é cada um destes ataques.

[ESPIONAGEM CIBERNÉTICA E GUERRA CIBERNÉTICA]

A **espionagem cibernética** afeta não só governos ou autoridades públicas, mas também empresas privadas. Os chamados ataques dirigidos ou APTs (*Advanced Persistent Threats* ou "ameaças persistentes avançadas") são projetados especificamente para uma entidade específica e um de seus principais objetivos é obter informações confidenciais com um propósito financeiro ou de espionagem industrial ou política.

Em 2012, a Saudi Aramco, a maior petrolífera do mundo, sofreu um dos piores ataques[4] de **espionagem cibernética industrial** da história da segurança cibernética. Cerca de 30.000 computadores e 2.000 servidores ficaram inacessíveis em questão de horas. O ataque foi lançado por um e-mail que continha um link que baixava um software mal-intencionado, e que se expandiria para o resto da rede silenciosamente para atacar de forma simultânea durante o Ramadã, quando a maioria dos funcionários da empresa estava em férias. A Saudi Aramco embarcou novamente no mundo do papel e do fax e não foi capaz de controlar a compra/venda de petróleo por meses, decidindo, após algum tempo, dá-lo de presente para não parar a produção, com as consequentes perdas milionárias que isso representou para a empresa. O ataque foi organizado por um grupo autodenominado *Cutting Sword of Justice* ("Espada Cortante da Justiça"), que fez menção ao apoio da Saudi Aramco ao regime político da família real da Arábia Saudita.

No caso da guerra cibernética ou **ciberguerra**, que vai além da mera espionagem industrial, temos o exemplo do "Stuxnet". Ele surgiu em 2010 e ficou conhecido na época como o *malware* mais inteligente já criado e foi desenvolvido para os sistemas industriais de tipo SCADA. Ele foi concebido com o objetivo de atacar as usinas nucleares no Irã, conseguindo atrasar em 10 anos a fabricação de urânio enriquecido nesses locais. Acredita-se, pelos indícios encontrados no código-fonte, que foi desenvolvido conjuntamente pelos Estados Unidos e Israel e que foi um trabalho de mais de um ano realizado por uma equipe de especialistas. Não foi um brinquedo desenvolvido por um mero amador.

[MALWARE]

No caso de *malware* ou software mal-intencionado, podemos distinguir entre as variantes que tentam se passar por um "programa legítimo", tratando de roubar a identidade de alguma entidade, e as variantes que restringem o acesso a determinadas partes do sistema operacional, codificando seus arquivos e pedindo um resgate em troca, o que tecnicamente se conhece como *ransomware* (do inglês *ramson,* resgate, e *ware,* programa).

Um exemplo de *malware* de roubo de identidade seria o conhecido como "vírus da polícia", do qual falaremos mais adiante, na seção sobre Engenharia Social. Quanto à segunda variante, quem não sofreu ou conhece alguém com um dispositivo que tenha sido infectado com um "vírus" que codificou todos os seus arquivos e que não permite fazer nenhuma ação no sistema? O ***malware*** do tipo *cryptolocker* está sendo uma das piores dores de cabeça para os equipamentos de segurança e suporte a usuário nas empresas. As equipes de operações precisam estudar todo o ciclo de infecção, desde que o *malware* é recebido (geralmente por e-mail) até sua detecção e, desde que os sistemas são infectados, colocados em quarentena e corrigidos por meio de recuperação de cópias de segurança ou *backups* do sistema, já que alguns destes "vírus" são praticamente impossíveis de remover e é preciso restaurar o sistema para um estado anterior. Outra opção que temos para eliminá-lo é pagando os "bandidos", mas desta forma estaríamos colaborando diretamente com o crime cibernético.

Este tipo de fraude é conhecido como *Crimeware* (ou "programas criminosos") pelo fato de comprometer sistemas de usuário ou de servidores usando software mal-intencionado, incluindo *phishing.* Por meio de portais aparentemente confiáveis de websites, os "bandidos" buscam dados de usuários, senhas, informações de pagamentos, etc. Eles têm como objetivo roubar a identidade de uma organização (geralmente *sites* de banco) a fim de obter uma recompensa financeira. Às vezes, os ataques são muito sofisticados, mas em outros casos são fáceis de detectar.

Existe uma variante deste tipo de *t* por exemplo, onde se pede ao usuário todos os números de cartão de banco e depende da ingenuidade da vítima morder ou não a isca.

Ilustração 1. Exemplo de *Phishing* Bancário

[TPVS E CÓPIA DE CARTÕES DE CRÉDITO]

Quando falamos de ataques a **Pontos de Venda (TPV) ou *Point of Sales (PoS)***, os atacantes tentam comprometer servidores ou os dispositivos de PoS para obter informações de pagamento. As empresas que mais sofrem este tipo de ataque são as de vendas ao consumidor comum como as do setor de hotelaria. Outra ameaça relacionada é a instalação de terminais falsos nos caixas automáticos para roubo de cartões de crédito, o que afeta principalmente os bancos. e das transações realizadas com cartões de crédito o que afeta principalmente os bancos.

Para evitar este tipo de fraude, as empresas Visa e MasterCard criaram uma norma de cumprimento obrigatório (PCI-DSS) para aumentar a segurança dos dados e das transações realizadas com cartões de crédito que afeta todas as empresas (e lojas) que processam, transmitem e/ou armazenam esses dados.

[WEBSITES]

Os **ataques a websites** baseiam-se principalmente em comprometer credenciais de usuário usando força bruta ou roubo e/ou em explorar vulnerabilidades no software ou na infraestrutura que lhes dá suporte, tais como gestores de conteúdos ou plataformas de comércio eletrônico. A maioria das empresas coloca à disposição de seus clientes e funcionários as plataformas de websites necessárias para o negócio, mas que podem colocar as informações da empresa em risco.

[RECUSA DE SERVIÇO]

Nos últimos anos, as empresas têm sofrido vários **ataques de Recusa de Serviço Distribuídos,** conhecidos como DDoS (do inglês, *Distributed Denial of Service)*. Nas notícias, já ouvimos falar de ataques de organizações *hacktivistas,* como a Anonyumus e a LulzSec, que deixaram sem conectividade ou desativado um site de uma empresa. Isso geralmente se consegue por meio de ataques DDoS e com o intuito de obter um dano à reputação. Para executar este ataque, infecta-se um grande número de computadores conectados à rede para obter suficientes recursos e conseguir que o ataque seja bem sucedido. Desta forma, eles formam o que se denomina uma *botnet,* ou uma rede de computadores infectados ou *bots.* Na hora do ataque, usam-se todas as máquinas infectadas para gerar um número enorme de conexões simultâneas para um objetivo específico: o site da empresa em questão.

[VAZAMENTO DE INFORMAÇÃO]

O vazamento de informação é uma das ameaças mais importantes para uma organização. O **uso indevido** dos sistemas de organização e seus dados, a **perda de dispositivos** ou de informação impressa, a falta de controle de acesso nas instalações ou os **erros diversos** (como divulgar dados confidenciais em uma rede pública ou enviar um email a destinatários errados) poderiam comprometer as informações da organização. Sem uma gestão adequada destas ameaças, poderíamos acarretar graves multas quando se trata de dados de alto nível de segurança conforme as normas de proteção de dados, como, por exemplo, dados pessoais ou de saúde.

ENGENHARIA SOCIAL

Um dos maiores desafios das equipes de segurança da informação das empresas é a engenharia social. As técnicas de **engenharia social** manipulam o usuário por meio da psicologia e as habilidades sociais do invasor para obter as informações que deseja da vítima, o que poderá variar entre saber qual é seu usuário e senha, obter acesso a áreas restritas ou conseguir dinheiro em troca de algo que nunca chegará. As técnicas de engenharia social são cada vez mais sofisticadas e mais difíceis de detectar. Os criminosos cibernéticos já não precisam desenvolver aplicações complexas, e sim enfocar a pessoa, que é o elo mais fraco da cadeia do ponto de vista da segurança. Os criminosos cibernéticos confiam na manipulação psicológica para estimular a vítima a fazer coisas que normalmente não faria, obtendo delas informações realmente valiosas.

Muitos dos ataques mencionados anteriormente, como o *cryptolocker* e o *phishing* bancário, são exemplos de *malware* que usa técnicas de engenharia social. Um exemplo disso é o que ficou popularmente chamado de "vírus da polícia". Este tipo de vírus tenta impressionar suas vítimas, fazendo-as acreditar que eles cometeram um crime (propriedade intelectual, pornografia, pedofilia, direitos autorais, etc.) e coloca gentilmente à disposição delas um método de pagamento fácil e simples para resolver o crime "cometido".

Ilistração 2. Vírus da polícia

Estes ataques são muito difíceis de superar, uma vez que envolvem diretamente as pessoas. A melhor **contramedida** para isto é a divulgação, conscientização e formação dos usuários para que saibam da existência deste tipo de técnica e consigam se defender.

OS "BANDIDOS" E SUAS VÍTIMAS

E quem são estes **"bandidos"?** São os novos abigeatários ou ladrões de gado da rede: máfias organizadas vindas do mundo inteiro cujo *malware* se origina essencialmente em países do leste europeu e em países asiáticos que se dedicam à criação deste tipo de software com o objetivo de obter informações ou dinheiro de forma ilícita. É muito complicado o trabalho dos órgãos de segurança do Estado para prender estes bandidos que jogam basicamente com dois fatores: **distância/fronteiras e anonimato na rede.** Às vezes eles operam com o intermédio de "mulas", que nada mais são que meros intermediários que fazem o "trabalho sujo". Estas máfias organizadas contratam pessoas por meio de ofertas de trabalho, fazendo-os acreditar que vão cooperar em planos estratégicos de multinacionais e que podem conseguir dinheiro rápido e fácil. Seu trabalho vem a ser o de transportar a mercadoria ou o dinheiro de um local para outro, e desta forma se perde a rastreabilidade e a perseguição dos bandidos fica complicada.

Nem todos os ataques são de máfias organizadas; muitos são produzidos por **pessoal interno,** conhecido como *insiders,* que conhecem e dominam o cenário, razão pela qual o ataque pode ser muito mais prejudicial do que quando se trata de atores externos. Também há o perfil do ***hacktivista*** que mencionamos anteriormente, motivado por uma ideologia específica e que faz ataques com uma finalidade específica. Por último, temos outro tipo de perfil quando falamos de guerra cibernética, como é o caso, de um lado, dos **Estados,** e do outro, dos **terroristas.**

As **vítimas** desses ataques poderiam ser nós mesmos. Todas as indústrias e negócios estão em risco. Embora achemos que o risco de ataque externo não é alto, haverá sempre o risco de um ataque interno ou de os usuários fazerem mau uso dos sistemas e exporem informações confidenciais ao público. A verdade é que o público-alvo mudou das grandes empresas para as PMEs, ou pequenas e médias empresas, o que está elevando o número de ataques cibernéticos exponencialmente. Há ataques desde a entidades e administrações públicas até a setores como o farmacêutico, hoteleiro ou de vendas ao varejo.

No ano passado o número de criminosos cibernéticos foi ultrapassado em mais de 70.000, e isso provocará perdas, como comentamos no início do artigo, de mais de 14 bilhões de euros em 2015. Podemos dizer que o crime cibernético move mais dinheiro que o tráfico de drogas[5] nos últimos tempos.

E por que os chamamos de "bandidos" quando popularmente são conhecidos como "hackers"? É importante dizer que a palavra *hacker* se desvirtuou com o passar do tempo: o que nos anos 80 se conhecia como pessoas habilidosas com computadores e que eram capazes de fazer qualquer coisa com eles por diversão hoje ficou associado a "piratas tecnológicos", como introduziu o dicionário RAE em outubro de 2014. Na época, essa acepção provocou duras críticas pelo grupo de peritos em segurança por não ter sido associada também a seu significado de origem. Seria mais correta a denominação de *cracker* ou *criminoso cibernético.*

O QUE POSSO FAZER PARA GERENCIAR O RISCO EM MINHA EMPRESA

O combate no devido tempo e forma às principais ameaças que enfrentamos pode ser um elemento diferencial e definitivo na continuidade e sustentabilidade do nosso negócio. É necessário definir uma estratégia próativa, ao invés de agir somente quando os acidentes acontecem. Mais cedo ou mais tarde nossa empresa será atacada.

O risco, por sua própria natureza, não pode ser eliminado, mas podemos, sim, desenvolver contramedidas para reduzi-lo, tanto em nível jurídico quanto organizacional e técnico. O êxito na redução do risco a que estamos expostos depende de dois **pilares: governança e segurança tecnológica.** De um lado temos o quadro normativo, legal e jurídico, o estabelecimento de políticas de segurança adequadas e boas práticas nas empresas e, do outro, a segurança tecnológica. O intuito destes pilares básicos é a proteção dos ativos da empresa, com destaque para "as pessoas" como o ativo mais importante.

No tocante à **governança da segurança,** devemos considerar diversos fatores. É imprescindível conhecer, em primeiro lugar, a fome de risco da empresa e contextualizá-la com o quadro legal e jurídico do país: normas relacionadas à proteção de dados, normas relacionadas ao terrorismo cibernético, normas de saúde e financeiras ou do nosso setor de atividade. Na mesma linha, temos que estabelecer em nossa empresa a políticas empresariais e de segurança adequadas, bem como desenvolver um código de conduta e investir na divulgação e conscientização, para que todos os usuários da empresa estejam cientes dessas normas. Um estudo da *Enterprise Management Associates* apontou que apenas 56% dos funcionários tinha recebido alguma tipo de formação em segurança, protocolos ou políticas.

No campo da **segurança tecnológica,** distinguimos entre a segurança lógica ou da informação e a segurança física. Temos de trabalhar dentro de nossa empresa em questões-chave como gerir uma infraestrutura de segurança adequada, instaurar uma equipe adequada de resposta a incidentes e dispor de controles de segurança física adequados nas instalações da nossa empresa. As equipes de resposta a incidentes prestam serviço por meio de Centros de Operações de Segurança e são consideradas CERTs *(Computer Emergency Response Team* ou "Equipe de Resposta a Emergências em Computação"), como parte da rede de CSIRTs mundiais *(Computer Security Incident Response Team* ou "Equipe de Resposta a Incidentes de Segurança da Computação"). Alguns dos mais conhecidos nacionalmente (na Espanha) são o CCN-CERT do Centro Criptológico Nacional ou o CERT de Segurança e Indústria operado pelo INCIBE (Instituto Nacional de Segurança Cibernética), que trabalha para a proteção das mais importantes infraestruturas nacionais e na luta contra o crime e o terrorismo cibernéticos, entre outros. Este tipo de instituição em nível governamental (existentes em outros países) concentra seu trabalho essencialmente na salvaguarda do estado de bem-estar do país. Na Espanha, em particular, as atividades realizadas por estes centros são parte da **Estratégia de Segurança Cibernética Nacional.**

Como recomendação final, gostaríamos de salientar que é essencial estar atualizado em segurança, o que vale não só para as equipes especializadas, mas para todos os funcionários de uma empresa. Os usuários da organização precisam conhecer os riscos a que estão expostos e a capacidade de geri-los de uma forma ou de outra. Um dos produtos que está se proliferando nas empresas são os seguros em **segurança cibernética,** que tratam de dar uma resposta ante um desastre cibernético e reputacional. Uma vez que os riscos tenham sido minimizados, o risco residual latente é transferido por meio de apólices específicas de riscos cibernéticos. Destacaríamos o famoso caso da SONY de 2011, de quem chegaram a roubar mais de 25 milhões de contas que continham cerca de 18 mil cartões de crédito e contas bancárias pela *Play Station Network.*

Em suma, há que projetar uma estratégia de segurança contínua, persistente e sustentável, dispor de sistemas e infraestruturas atualizados e investir coerentemente em segurança cibernética para assegurar as infraestruturas da empresa e garantir o sucesso e a continuidade da nossa empresa.

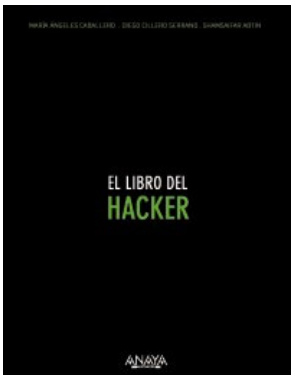
A MAPFRE E SUA CONTRIBUIÇAO AO MUNDO DA SEGURANÇA DA INFORMAÇÃO

A MAPFRE, como uma empresa comprometida com a sociedade, trabalha contínua e ativamente na proteção dos interesses de seus clientes, funcionários, acionistas e fornecedores prevenindo e detendo incidentes de segurança.

Este trabalho contínuo é realizado por sua equipe de especialistas em segurança cibernética da **Direção Corporativa de Segurança e Meio Ambiente** e sua **Equipe de Resposta a Incidentes de Segurança da Informação,** conhecido como o **CGC-CERT.** A equipe de resposta a incidentes da MAPFRE dispõe de um sofisticado laboratório e um grupo de profissionais altamente qualificados incumbidos de prevenir, responder e minimizar o impacto de possíveis incidentes de segurança. No contexto global e multinacional da MAPFRE o trabalho do CGC-CERT não é meramente interno. Há uma colaboração ativa com outras empresas e instituições tanto nacional quanto internacionalmente.

BIBLIOGRAFÍA RECOMENDADA: EL LIBRO DEL HACKER, DA ANAYA

Para quem deseja adentrar o mundo da segurança da informação ou se aprofundar no assunto do artigo, recomendamos **El Libro del Hacker,** da editora ANAYA. O livro aborda questões de segurança, desde capítulos introdutórios à insegurança da informação até as técnicas de ataque mais sofisticadas, desde seus estágios iniciais *(footprinting/fingerprinting),* passando por suas etapas mais avançadas *(exploiting)* e exclusão de provas. Também podemos encontrar outros temas atuais como segurança em redes sociais, computação em nuvem, gerenciamento de identidades, ameaças cibernéticas, etc.



É um livro que pode ajudar tanto as pessoas que estiverem interessadas em entrar no mundo da segurança da informação como especialistas mais avançados. Sua ficha editorial completa pode ser consultada no site da editora: http://www.anayamultimedia.es/libro.php?id=3608921

[1] "Cyber Catastrophe" *working paper, University of Cambridge Judge Business School*
[2] "Verizon Data Breach Investigation Report" (DBIR) – 2014
[3] "España, a la cabeza del cibercrimen" Diario ABC – 2015
[4] "Arabia Saudí dice que el ataque informático contra Aramco fue lanzado desde el exterior" El País http://economia.elpais.com/economia/2012/12/09/agencias/1355069609_526898.html
[5] La ciberdelincuencia mueve más dinero que el narcotráfico en el mundo http://www.abc.es/espana/20141207/abci-ciberdelincuencia-dinero-201412062106.html