01

© Nicolau

Cyber attack methods and business impact

Métodos de ciberataque e impacto nos negócios

Ernest Legrand, Chief Executive Officer at New York-based technology company WEBCBG and a Specialized Resource Member of Brokerslink, advises business leaders to address cyber risk and take active steps to identify, assess and manage the risk on an enterprise wide basis.

Ernest Legrand, CEO da empresa de base tecnológica sediada em Nova Iorque WEBCBG, e Specialized Resource Member da Brokerslink, aconselha os responsáveis das empresas a encarar o risco cibernético e a agir ativamente, tomando medidas para identificar, avaliar e gerir o risco de forma transversal nas empresas.

When Jimi Hendrix sang Elmore James' *Bleeding Heart*, little did he know that he would be a victim of copyright theft after his death in 1970. The song portrayed desolation and heartbreak and today the Heartbleed Bug that left 300,000 web servers vulnerable in 2014 ironically conveys the same message. The bug along with scores of cyber-attack methods threatens to bleed out hundreds of millions of dollars from businesses and government enterprises across nationalities causing much anxiety and despair. The enduring Shellshock bug makes 70% of all machines vulnerable and has been going undetected for the last 20 years.

With 120,000 incoming cyber attacks every day growing at 60% annually it is no surprise that cyber security is quickly gaining prominence within IT budgets and enterprise risk management programs.

Quando Jimi Hendrix cantou *Bleeding Heart* de Elmore James, estava longe de imaginar que viria a ser vítima de usurpação de direitos de autor após a sua morte em 1970. A canção falava de desolação e desgosto, e o *Heartbleed Bug*, que em 2014 colocou 300 000 servidores da Internet em situação de vulnerabilidade, veicula, ironicamente, a mesma mensagem. Juntamente com inúmeros outros métodos de ciberataque, este *bug* ameaça desviar centenas de milhões de dólares de empresas e instituições governamentais de diferentes nacionalidades, provocando grande preocupação e ansiedade. O resistente *Shellshock Bug* afeta de cerca de 70 % das máquinas em termos de vulnerabilidade e tem permanecido indetetável nos últimos 20 anos.

Com 120 000 novos ciberataques por dia, e um crescimento anual de 60%, não é de surpreender que a cibersegurança comece a adquirir uma crescente importância nos orçamentos das áreas das Tecnologias de Informação (TI) e nos programas de gestão do risco das empresas. Em 2013, 3000 empresas norte-americanas não tinham conhecimento de que estavam a ser alvo de intrusões cibernéticas até serem notificadas nesse sentido pelo FBI e, em 2014, as organizações que sofreram quebras de segurança registaram uma média anual de perdas pecuniárias de cerca de 400 000 dólares.

Os riscos cibernéticos não se limitam apenas a grandes empresas, infraestruturas críticas, governos ou grandes cadeias de abastecimento; ninguém está a salvo. Como poderão as empresas enfrentar a necessidade urgente de um programa sólido de segurança cibernética? Apesar de existirem vários frameworks de qualidade, a maior parte começa pela classificação e identificação de métodos de ciberataque que são decisivos para a análise da motivação e para a mitigação dos danos. Quer se trate de incidentes patrocinados por Estados, propaganda, atos criminosos em si, ou levados a cabo por *hactivists* (*hackers* ativistas), o custo anual da cibercriminalidade para a economia global é de 300 a 500 mil milhões de dólares, na estimativa da McAfee. A gravidade do problema esteve na origem da "Executie Order" do Presidente dos EUA de 2013, e da criação do *Cyber Security Framework*, pelo National Institute of Standards and Technology (NIST).

Infelizmente, o panorama da cibercriminalidade não se limita apenas ao roubo organizado, tendo igualmente a ver com uma crescente complexidade e técnicas sofisticadas. Um mapeamento dos principais ciberataques identifica combinações criativas de métodos cibernéticos conhecidos, designadamente os seguintes: (1) *Malware*: vírus, *worms*, cavalo de Tróia, *spyware*, *adware*, *scareware*; (2) Injeção de SQL: comandos SQL; (3) *Spear phishing*: *e-mails* fraudulentos; (4) DDoS: ataques que bloqueiam a disponibilidade de serviços na rede, no sistema ou *on-line*; (5) Ataques XSS: *scripts* maliciosos escondidos em *websites*; (6) *Watering Hole*: ataque oportunístico através da introdução de um código malicioso numa página na Internet; (7) APT ou "Advanced Persistent Threat": ataque persistente, implacável e indetetável visando dados confidenciais ou propriedade intelectual, sendo a operação de deteção e recuperação dispendiosa.

In 2013, 3,000 US companies were unaware of cyber intrusions until notified by the FBI, while for organizations with security incidents the average annual monetary loss was approximately $400,000 in 2014.

Cyber exploits are not limited to large businesses, critical infrastructure, government or large supply chains, anyone and everyone are at risk. How then can businesses address this pressing issue of a robust cyber security program? Though there are several good frameworks available most start with first step as classification and identification of cyber-attack methods that are key to analyzing motives and damage mitigation. Whether incidents are state sponsored, propaganda or criminal by nature or by hactivists, the annual cost to the global economy from cybercrimes is between $300 and $500 billion as estimated by McAfee. The gravity of this issue prompted US President's 2013 Executive Order on improving cyber security and the formation of the National Institute of Standards and Technology (NIST) Cyber security Framework.

Unfortunately cybercrime landscape is not just about organized theft, it is also about increasing complexity and sophisticated techniques. A mapping of the major cyber-attacks identifies creative combinations of well--known cyber methods such as: (1) Malware: Virus, worms, Trojan horse, spyware, adware, scareware; (2) SQL Injection: Malicious SQL commands; (3) Spear phishing: Targeted email scam; (4) DDoS: Attack on Network, system or online service availability; (5) XSS Attacks: Malicious scripts on web sites; (6) Watering Hole: Opportunistic attack through a malicious code on a webpage; (7) APT or "Advanced Persistent Threat": A persistent relentless and undetected attack targeting sensitive data or intellectual property, making recovery and detection a costly proposition.

The severity of sophisticated attacks can be understood from the fact that Adobe had its 150 million customer data compromised in 2013 as an effect of Malware and APT injected into its systems. Target Inc. also paid the price with personal information of 70 million people and card data of 40 million compromised in a combined APT, malware and spear phishing attack. JP Morgan suffered from a three month undetected cyber-attack giving hackers the highest level of administrative privileges on more than 90 of the bank's servers in 2014. Consequently data pertaining to 76 million households and 7 million small businesses was breached. Astonishingly nine other financial institutions were also attacked by the same group said to be originating from Russia.

New technologies have fuelled new attack tactics. Point of Sale systems, Digital payment systems, Internet Of Things, Clouds and Mobility have added new dimensions with rising worms and viruses making way through vulnerable systems.

No matter what methods are used whether external or internal, on desktop or mobile systems, businesses today are challenged with maintaining corporate credibility and securing sensitive data with major cost implications after a cyber attack. Lost business and erosion of customer trust can

have enduring consequences on brand image and company reputation that are built over years, while governmental enterprises have to face damaging consequences of cyber espionage threatening national utilities or even national security. Ransomware is the new trend of cyber-attacks that threaten individual users and enterprises altogether with ransom for the recovery of their own data.

Businesses today need to understand how key preventive measures can be implemented through an organizational cyber security framework to address cyber crime. A stepwise approach to forming a strategy would include:

1. Commission an IT system vulnerability assessment to identify and evaluate inside and outside sources including contractors, third party vendors, and employees.
2. Define day-to-day security procedures
3. Secure IT systems:
   a. Activate firewall
   b. Test vendor systems before giving access to the internal network
   c. Use latest versions of anti-virus, anti- spyware software
   d. Test mobile devices for vulnerabilities
   e. Monitor internet connection
4. Use "white hat"[1] hackers to test the implementation
5. Set up intellectual property agreements
6. Execute regular system updates and turn on automatic updates for all Operating Systems
7. Update and evaluate commonly used software: Java, Adobe Reader, Microsoft Office, Flash, Internet Explorer: all have carried vulnerabilities at one stage or the other
8. Change passwords frequently and stay cautious while using public computers
9. Never click on email links or download attachments without verifying authenticity
10. Ensure the senior management regularly communicate to the employee on safe cyberspace behavior and security awareness training

According to recent surveys, best practices such as IT system vulnerability assessment, account/ password-management policy, cyber risks inclusion in enterprise risk-management program, intrusion detection system have been reported as successful deterrents by governmental organizations.

A gravidade destes ataques sofisticados pode ser demonstrada pelo facto de, em 2013, a Adobe ter visto comprometidos os dados de 150 milhões dos seus clientes como resultado de *malware* e APT injetados nos seus sistemas. A Target Inc. também teve de pagar um preço elevado pelo facto de dados pessoais de 70 milhões de pessoas e de os dados de 40 milhões de cartões terem ficado comprometidos na sequência de um ataque que combinou APT, *malware* e *spear phishing*. Em 2014 a JP Morgan foi alvo, durante três meses, de um ciberataque não detetado que conferiu aos *hackers* o mais elevado nível de acesso a mais de 90 dos servidores do banco. Consequentemente, foi violada a confidencialidade dos dados de 76 milhões de famílias e de sete milhões de pequenos negócios. Surpreendentemente, nove outras instituições financeiras foram também alvo de ataque pelo mesmo grupo, alegadamente originário da Rússia.

Novas tecnologias têm permitido novas táticas de ataque. Sistemas de ponto de venda (POS), sistemas de pagamento digital, a Internet das Coisas, a computação em nuvem e a utilização de suportes móveis têm acrescentado novas dimensões, com um número crescente de *worms* e vírus penetrando em sistemas vulneráveis.

Independentemente dos métodos utilizados – externos ou internos, em *desktop* ou sistemas móveis – as empresas são hoje confrontadas com a necessidade de manter a credibilidade corporativa e de proteger dados confidenciais, com enormes consequências no que diz respeito aos custos após um ciberataque. A perda de negócio e a diminuição da confiança dos clientes podem ter consequências duradouras para a imagem da marca e para a reputação da empresa, construídas ao longo dos anos, enquanto as entidades governamentais têm de enfrentar as consequências nocivas da ciberespionagem que constitui uma ameaça para os serviços públicos ou mesmo para a segurança nacional. O *ransomware* é a nova tendência de ataque cibernético que ameaça tanto os utilizadores individuais como as empresas com pedidos de resgate para a recuperação dos seus próprios dados.

Para se protegerem da cibercriminalidade, as empresas de hoje precisam de compreender de que forma poderão implementar medidas preventivas através de um sistema organizativo de cibersegurança.

Ernest Legrand
CHIEF EXECUTIVE OFFICER AT WEBCBG

The company focus areas include advanced software development leveraging big data analytics and data visualization techniques in the insurance industry, as well as mobile application and digital marketing. WEBCBG has recently released Glossarisk, the first insurance glossary on mobile devices, in association with IRMI (International Risk Management Institute). To bring the greatest value to clients and provide competitive advantage, WEBCBG utilizes the latest technologies in a cloud computing environment to develop powerful and sophisticated capabilities that were only affordable to large enterprises until recently. Prior to joining WEBCBG, Ernest was a senior executive at IBM. He was Vice President of Global Marketing & Strategy for IBM in the Insurance and Banking industries for 6 years and then was appointed Vice President Global Marketing & Strategy for ibm.com, the IBM corporate portal over 96 countries. He was also the Chair of the IBM Web Community worldwide. He has executed numerous Internet campaigns and created Web content organizations around the world. Part of his responsibilities included the IBM Web user experience, the traffic generation and the level of client services. Before joining the global business operations, Ernest was Director of IBM Corporate Internet strategy responsible for designing and implementing Web strategies to transform IBM into the world's premier e-business. He owns a patent on push technology used by IBM sales organizations. Earlier in his career, Ernest was Chief Marketing Officer and Member of the Board at CGI, one of the largest Software and Services Company in Europe.

As áreas de atividade core da empresa incluem o desenvolvimento de software avançado, para aproveitamento de análises de big data e de técnicas de visualização de dados, no setor dos seguros; bem como aplicações móveis e marketing digital.
A WEBCBG lançou recentemente, em associação com o IRMI – Instituto Internacional de Gestão de Risco, o Glossarisk, o primeiro glossário de seguros para dispositivos móveis.
Para reforçar o valor oferecido aos clientes e conseguir uma vantagem competitiva, a WEBCBG utiliza as mais recentes tecnologias num ambiente de computação 'na nuvem', de modo a desenvolver capacidades reforçadas e sofisticadas que, até recentemente, estavam apenas acessíveis às grandes empresas.
Antes de se juntar à equipa da WEBCBG, Legrand era executivo sénior na IBM. Ao longo de seis anos, foi vice-presidente da área de marketing global e estratégia na IBM, para os setores dos seguros e da banca. Foi depois nomeado vice-presidente da área de marketing global e estratégia na ibm.com, no portal corporativo da IBM para 96 países. Foi também presidente mundial da comunidade da IBM na Web. Executou várias campanhas na Internet e criou redes de conteúdo Web em todo o mundo. Nas responsabilidades que então assumiu incluía-se a experiência do utilizador do site da IBM, a geração de tráfego, e o nível de qualidade dos serviços prestados aos clientes. Antes de integrar a área comercial, Legrand foi diretor da estratégia corporativa da IBM para a Internet, cargo em que se responsabilizou pela conceção e implementação de estratégias Web para tornar a IBM na principal empresa de e-business do mundo. Legrand detém uma patente sobre a tecnologia push, utilizada pela força de vendas da IMB.
No início da sua carreira, Legrand foi diretor de marketing e membro do Conselho de Administração da CGI, uma das maiores empresas de software e serviços na Europa.

Uma abordagem faseada para delinear uma estratégia de cibersegurança incluirá:

1. efetuar uma análise da vulnerabilidade do sistema de TI para identificar e avaliar as fontes internas e externas, incluindo adjudicatários, fornecedores subcontratados, e empregados;
2. definir procedimentos de segurança no dia a dia;
3. proteger os sistemas de TI:
   a. ativar *firewalls*,
   b. testar os sistemas dos fornecedores antes de lhes dar acesso à rede interna,
   c. utilizar as versões mais atualizadas de *software* antivírus e *antispyware*,
   d. testar a vulnerabilidade dos dispositivos móveis,
   e. monitorizar a ligação à Internet;
4. utilizar *hackers* 'de chapéu branco'[1] para testar a implementação;
5. celebrar acordos de proteção da propriedade intelectual;
6. executar atualizações periódicas do sistema e ativar atualizações automáticas para todos os sistemas operativos;
7. atualizar e avaliar o *software* mais utilizado: Java, Adobe Reader, Microsoft Office, Flash, Internet Explorer: todos estes programas revelaram vulnerabilidades, em determinada altura;
8. alterar frequentemente as palavras-passe e manter uma atitude prudente ao utilizar computadores públicos;
9. nunca clicar em hiperligações de *e-mail* nem efetuar o *download* de anexos sem verificar a sua autenticidade;
10. assegurar a existência de informação frequentemente aos colaboradores, por parte da administração e direção da empresa, sobre comportamento seguro no ciberespaço e sobre programas de sensibilização para a segurança.

Estudos recentes revelam que boas práticas, tais como a avaliação da vulnerabilidade dos sistemas de TI, uma política de gestão de contas / palavras-passe, a inclusão de riscos cibernéticos nos programas de gestão do risco, ou a adoção de sistemas de deteção de intrusões, têm sido consideradas como medidas preventivas de sucesso nas organizações governamentais.

1 Nota do tradutor:
"white hat" também designados por "ethical hackers" (hackers éticos), atuam com vista à proteção da empresa.