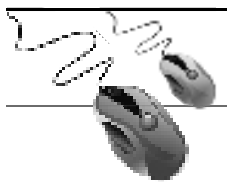


Ciência e Tecnologia

ricardosouza@netjen.com.br

www.netjen.com.br

Tech's up! Por mais mulheres na área da tecnologia

Luciana Carvalho (*)

Há mais ou menos 2 meses estava junto com algumas amigas assistindo o filme "Estrelas Além do Tempo". O filme, baseado em um livro de não ficção, conta a história de três mulheres que tiveram importância fundamental no programa espacial americano, em uma época em que as tensões entre os Estados Unidos e a União Soviética atingiram seu ápice

Inevitavelmente o filme também traz uma reflexão acerca da escassez de mulheres no segmento de ciências e tecnologia. Ainda que tenhamos a oportunidade de ver mais mulheres à frente de grandes empresas e trazendo perspectivas e estilos de liderança diferentes (ainda longe do ideal), quando olhamos para o universo de tecnologia, a representatividade feminina ainda se revela bastante tímida.

Em um rápido retorno ao histórico da primeira turma de Computação do IME (Instituto de Matemática e Estatística da Universidade de São Paulo), me surpreende que 70% dos alunos eram mulheres. Na época, a computação era um desdobramento do curso de matemática, que tradicionalmente já era mais frequentado por mulheres. O que mudou de lá para cá?

Para responder a essa pergunta, faz bastante sentido que olhemos para a história e alguns dados para entendermos como este cenário foi sendo construído.

Em primeiro lugar, a disseminação global transformou a tecnologia em uma questão cultural que passou a ser influenciada ainda na infância, época em que as meninas começam a ser desestimuladas a seguir carreiras técnicas. Segundo o livro Unlocking the Clubhouse: Women in Computing ('Entrando no Clubinho: Mulheres na Computação'), da pesquisadora Jane Margolis, metade das famílias americanas decide colocar o computador no quarto do filho homem, gerando uma associação precoce que acompanhará as crianças até a fase adulta. Nas próprias escolas é possível perceber essa mesma falta de estímulo à aproximação da tecnologia, bem como o próprio reconhecimento das habilidades matemáticas nas meninas, que, inevitavelmente, passam a preferir outros tipos de carreiras.

Mesmo quando as mulheres decidem ingressar na faculdade em cursos nas áreas de Ciências, Tecnologia, Engenharia e Matemática, apenas 26% delas seguem carreira efetivamente na área, contra 40% dos homens (STEM). Isso significa que a maioria das mulheres qualificadas desistem de trabalhar nessas áreas, mesmo após estarem formadas e com conhecimento adquirido.

Entre as mulheres que finalmente decidem por carreiras técnicas na área de tecnologia, algumas pesquisa revelam que elas imediatamente encontram um ambiente de trabalho bastante desfavorável, com pouca diversidade e um excessivo comportamento machista e competitivo entre os colegas, o que desestimula a permanência nessas empresas.

Essa distorção marca a diferença atual entre as empresas de tecnologia e o resto do mercado de trabalho. No ranking das 100 maiores empresas do mundo, 20% têm, pelo menos, uma diretora. No Vale do Silício, esse número cai para 10% das empresas. De acordo com o Departamento de Trabalho dos Estados Unidos, apenas 11% dos profissionais de Engenharia do país são mulheres. Segundo um estudo da Harvard Business School, apenas 10% dos aportes financeiros na forma de investimentos são feitos em startups comandadas por mulheres. Nos Estados Unidos, as programadoras de código correspondem a 26% do total. No Brasil, a situação é ainda pior: apenas 17% dos programadores brasileiros são mulheres.

Essa matemática precisa mudar radicalmente. As empresas de tecnologia precisam compreender a importância de olhar a diversidade como um fator positivo. Pesquisa do Gallup aponta que corporações que apostam em perfis mais plurais – inclusive com mais mulheres – têm um turnover 22% menor e uma facilidade maior na hora de contratar; times de tecnologia com maior diversidade também tendem a ser mais eficientes e produtivos; empresas com profissionais de background diferentes representam melhor a própria sociedade, passam a compreendê-la melhor e desenvolvem a capacidade de produzir produtos e serviços mais adequados e pertinentes aos dias de hoje.

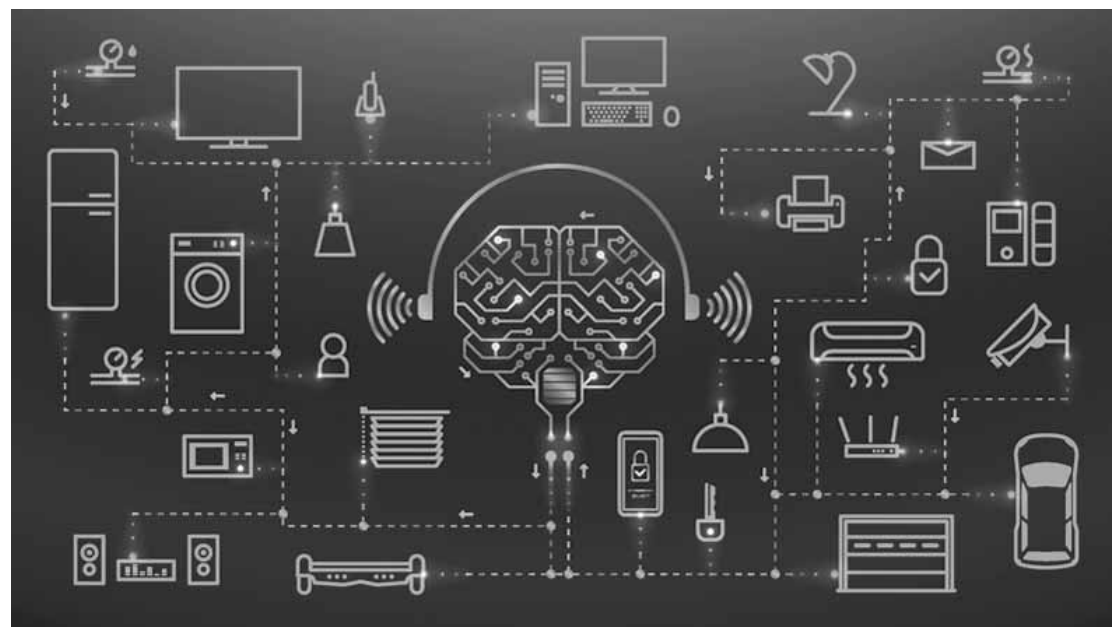
A verdade é que nós, profissionais em posições de liderança, devemos ajudar os gestores a preparar seus times para a diversidade. Isso deve ocorrer não apenas no momento da contratação, mas também de maneira constante, estimulando um ambiente de trabalho que respeite as individualidades. Mulheres têm o direito e a competência para exercer qualquer cargo em qualquer empresa, seja na área técnica, gerencial ou executiva. Precisamos de pessoas talentosas, homens e mulheres, que estejam prontas para assumir o protagonismo que seus cargos exigem, mas que também possam ajudar a construir um mundo mais aberto. Só depende de nós.

(*) É Diretora de Gente da Movile.

As atividades de exploração de IoT aumentaram quatro vezes

A evolução do malware está sendo em grande parte motivada pela proliferação da Internet das Coisas. De acordo com os dados do Gartner, existiam cerca de 8 bilhões de "coisas" conectadas em 2017

Anthony Giandomenico (*)



Mas esse número deve aumentar quase três vezes e ultrapassar 20 bilhões nos próximos dois anos, o que significa cerca de três dispositivos conectados por pessoa na Terra. Em outras palavras, a oportunidade para os cibercriminosos de entrar na rede e roubar dados ou manter segmentos da rede, ou a rede inteira, como refém está crescendo de forma exponencial, sem sinais de desaceleração.

O relatório da Fortinet sobre o cenário de ameaças publicado no quarto trimestre de 2017 confirma essa conclusão, principalmente no que se refere a explorações de IoT, que aumentaram quatro vezes nesse período. Durante o quarto trimestre de 2017, o FortiGuard Labs detectou uma média de 274 ataques por empresa, o que representa um aumento significativo de 82% em relação ao trimestre anterior. As descobertas deste relatório são baseadas nos bilhões de eventos e incidentes de ameaças coletados pela rede global de dispositivos e sensores da Fortinet implementados em ambientes de produção ao vivo.

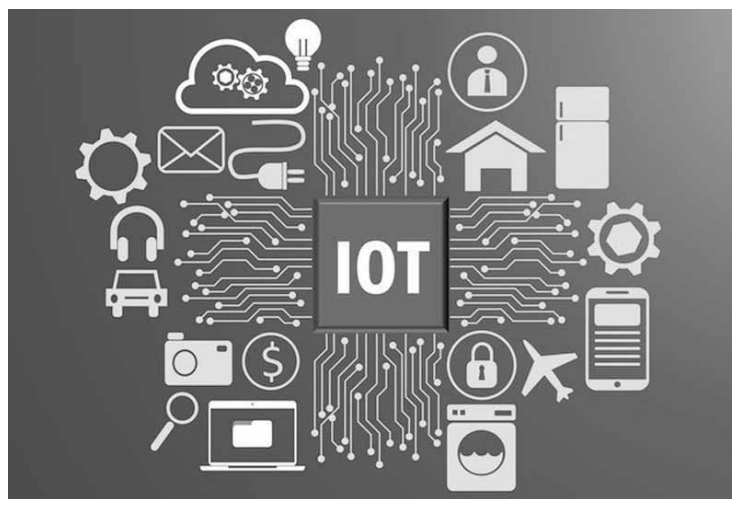
Ataques a dispositivos IoT em alta

Três dos 20 principais ataques identificados no quarto trimestre visaram dispositivos IoT. Ao contrário dos ataques anteriores à IoT, que exploravam apenas uma vulnerabilidade, os novos botnets de IoT, como o Reaper e Hajime, podem explorar várias vulnerabilidades simultaneamente. Esta abordagem de múltiplos vetores é muito mais difícil de combater. A estrutura flexível do Reaper, criada com scripts e mecanismo Lua, tem seu código facilmente atualizado, ao contrário dos ataques estáticos e pré-programados como as explorações IoT anteriores. Isso permite uma invasão mais rápida, executando ataques novos e mais mal-intencionados à medida que eles se tornam disponíveis em um botnet ativo já instalado.

O potencial deste tipo de evolução é alarmante. Por exemplo, o volume de exploração do Reaper no início de outubro aumentou de 50.000 para 2,7 milhões em apenas alguns dias e depois voltou ao normal.

O que vem pela frente

As consequências do aumento no número de ataques focados em IoT que visam dispositivos vulneráveis e sem correções provavelmente assumirão a forma de botnets enormes que vão piorar ainda mais o efeito de invasão generalizada observado no passado (por exemplo, os ataques causados pelo malware Mirai sofridos pela empresa Dyn). Essas "colmeias", ou hivenets, usam métodos de aprendizado de máquina e múltiplos vetores para identificar e atingir sistemas vulneráveis com supervisão humana mínima. Enquanto os botnets tradicionais aguardam comandos de um bot controlador, os dispositivos dos hivenets analisam um alvo, determinam suas possíveis vulnerabilidades e depois, operando de forma independente, escolhem a exploração mais provável para comprometer o alvo, espalhando-se com rapidez e causando os mais devastadores resultados.



Conforme descrito em nosso relatório Previsões para o cenário de ameaças de 2018, os hivenets poderão usar grupos de dispositivos comprometidos para identificar e assaltar diferentes vetores de ataque de uma só vez. À medida que identifica e compromete mais dispositivos, um hivenet poderá crescer de forma exponencial, ampliando sua capacidade de atacar várias vítimas simultaneamente, superando a capacidade das equipes de TI de aplicar correções ou novas assinaturas de prevenção de invasões ou antimalware. Portanto, é essencial que as organizações avaliem o que as atuais defesas de negação de serviço distribuídas podem gerenciar agora, para evitar problemas depois que um ataque do tipo "enxame" cruzar o seu caminho.

Proteger o que importa

Para se defender melhor contra as explorações da IoT, as práticas recomendadas começam com a identificação e o inventário dos dispositivos conectados à rede, documentando como eles estão configurados e controlando como eles se autenticam nos pontos de acesso da rede. Assim que tiver visibilidade completa, as organizações podem então segmentar de forma dinâmica os dispositivos IoT em zonas de rede protegidas com políticas personalizadas.

Porém, para uma segurança eficaz, será necessário vincular esses segmentos de maneira dinâmica usando um fabric de segurança integrado e automatizado que possa cobrir toda a rede, principalmente os pontos de acesso, e então verificar os segmentos do tráfego da rede movimentando-se lateralmente pela rede, mesmo na multinuvem.

O crescimento dramático das famílias de malware que visam a IoT ilustra a natureza incrivelmente prolífica dessa ameaça. A estratégia de "proliferar para penetrar" não é nova, mas é outro lembrete de que o antimalware de assinatura de ponto único simplesmente não consegue processar o volume, a velocidade e a variedade de malwares modernos. Para aumentar a proteção da rede e dos seus dados, as organizações precisam integrar as proteções de malware capazes de detectar ameaças conhecidas e desconhecidas nas várias camadas do ambiente de rede distribuído e dinâmico atual, desde os dispositivos de usuários até o núcleo e os ambientes na nuvem.

(*) É estrategista de Segurança Sênior da Fortinet.

A urgente preocupação com a proteção de dados nas redes sociais e a autodeterminação informacional

O fato recentemente descoberto da empresa de marketing político Cambridge Analytica - a qual conseguiu informações de mais de 50 milhões de usuários da rede social Facebook e, com isso, teria influenciado as eleições nos Estados Unidos da América e do Reino Unido - reascendeu o debate sobre a proteção de dados.

O assunto deve ser tratado com a maior urgência e preocupação possível. Em nossa sociedade da informação e de vigilância, a proteção de dados de usuários concerne a todos os envolvidos (usuários, plataformas, terceiros etc.). Trata-se de uma questão de segurança jurídica que afeta diretamente todos os cidadãos e, no campo, usuários da internet.

No campo jurídico, o Brasil carece de legislação apropriada. O Marco Civil da Internet de 2014 não trata de série de conceitos fundamentais na disciplina. Existem Projetos de Lei - o mais recente de 2016 - que tentam esboçar, ainda de maneira imperfeita, uma segurança mínima no tema.

Direitos da personalidade como intimidade e privacidade são aqui a pedra de toque. Quando uma pessoa cede um dado a certa plataforma, precisamos conhecer e reconhecer a extensão dos deveres e direitos deste responsável pelos dados.

Parece-me que o melhor seria considerarmos o assunto sob a ótica da doutrina e julgados alemães, muito mais afinados à nossa cultura do que propriamente o modelo de privacy estadounidense. Na Alemanha, é clara a presença do princípio da finalidade dos dados: somente pode ser requerido e mantido um dado em certa base conforme a finalidade a que ele presta. Existe relação inquebrável e civilizatória entre dado e sua finalidade: Zweckverbindung. Sem finalidade determinada, o dado não pode ser requerido; esgotada a finalidade, o dado deve ser apagado.

Na hipótese das redes sociais, existe Política de Privacidade que os usuários aderem. Existe prevalência nos estudiosos de que o consentimento para qualquer outra finalidade externa às redes sociais deva ser expresso e explícito. Porém, como se disse, o Brasil carece de legislação específica. O risco desta ausência já foi sentido em julgados europeus. Alguns permitiram o "vazamento" de dados para além das redes sociais, com base em comportamentos concludentes.

Às vésperas da entrada em vigor na Europa do novo Regulamento sobre o tema (em 25 de maio de 2018), denominado General Data Protection Regulation, é o momento mais adequado para o Brasil retomar a discussão do assunto de forma científica e profissional. Precisamos urgentemente de uma legislação afinada com o modelo da autoderminação informacional e fundada no princípio tanto da finalidade quanto do consentimento expresso dos usuários. Só assim conseguimos a segurança no tráfego de dados.

(Fonte: Rodrigo Vaz Sampaio é advogado e professor de Direito Civil e Proteção de Dados do CEU Law School).

News @TI

Na lista das 100 startups mais atraentes do Brasil

@A DogHero, plataforma que conecta mães e pais de cachorro a anfitriões que hospedam os pets em casa, é destaque na categoria serviços do ranking 100 Startups to Watch, que surge como um radar para orientar investidores, aceleradoras e programas de corporate venture. A análise, que durou mais de cinco meses, é resultado de uma parceria entre a revista "Pequenas Empresas & Grandes Negócios" e "Época Negócios", da editora Globo, e a Corp.vc, braço de corporate venture da consultoria EloGroup. Em três anos de história, a brasileira construiu uma base de 15.000 anfitriões em 650 cidades de todo o Brasil e mais de 1.100 em 20 cidades da Argentina. Até hoje, a startup levantou cerca de R$ 18 milhões em investimento com os fundos Monashees, com participação da Kaszek Ventures, Global Founders Capital (alemão) e IGNIA Partners (mexicano). Com três etapas, 1,3 mil empresas foram analisadas por consultores e especialistas da Corp.vc/EloGroup e da Editora Globo. Um grupo de 150 finalistas foi apresentado ao conselho consultivo que, por fim, definiu a lista das 100 que integram o ranking, que conta com 13 categorias: Agronegócio, Educação, Finanças, Gestão, Impacto, Indústria, Lazer e Turismo, Logística, Marketing, Moda e Beleza, Saúde e bem-estar, Serviços, Tecnologia da Informação e Realidade virtual (www.doghero.com.br).