



## É hora de incluir mais inteligência na segurança da informação

Jeferson Propheta (\*)

*Recentemente ataques cibernéticos sem precedentes nos colocaram em alerta e mudaram a forma como devemos lidar com a segurança da informação*

Os vazamentos de vulnerabilidades que forneceram as informações para que os ataques WannaCry e Petya fossem realizados, ainda serão bastante usados pelos cibercriminosos. Mais variantes do mesmo vazamento já foram detectadas e, considerando que mais de 30 vulnerabilidades foram publicadas, podemos esperar que ameaças nunca antes vistas sejam criadas a partir dessas informações.

O cibercrime avança rápido demais e já é impossível tentar combatê-lo apenas com a criação de mais e mais produtos de segurança. Ainda precisamos muito das ferramentas, mas sozinhas elas não podem resolver o problema. Além do que, é inviável para a maioria das empresas atualizar seu ambiente de segurança a cada novo produto promissor lançado, tanto pelo custo como pela demanda de esforços para gerenciar cada vez mais soluções.

O que fazer então para lidar com esse volume gigantesco de novas ameaças que surgem todos os dias? A resposta é incluir mais inteligência na estratégia de segurança e criar um plano de respostas a incidentes que correspondam às vulnerabilidades específicas de cada empresa.

Existem diversas ações que a equipe de segurança pode realizar que são bastante eficientes para combater as ameaças e que não dependem da implantação de uma solução

específica, ações como desligar algo no sistema operacional que impeça a propagação do malware, alterar configurações no sistema, habilitar alguma assinatura de proteção de rede ou bloquear alguma porta de comunicação.

No caso do WannaCry, por exemplo, foi usada exploração para protocolo SMB. Algumas empresas não precisam deste protocolo em todas suas operações e bastaria desabilitá-lo para bloquear a propagação do malware. Já as empresas que realmente precisam deste ou de outro protocolo, poderiam optar por soluções que realmente atuem prevenindo a exploração de vulnerabilidades, como virtual patching ou whitelist.

As equipes de segurança precisam receber mais informações do que oferta de produtos. O que vemos atualmente são equipes sobrecarregadas com o gerenciamento de muitas soluções e que muitas vezes nem sabem se tais soluções são essenciais para a defesa do ambiente. Cabe agora aos fornecedores de segurança compartilhar informações, informar o cliente sobre as tendências de ataques para cada tipo de mercado, novos malwares detectados, quais tipos de exploração estão acontecendo, e como mitigar, seja em rede, sistema ou aplicação.

Com a elaboração de um plano de respostas a incidentes mais inteligente e direcionado, as empresas conseguem de alguma maneira responder ao incidente; evitar que o ataque aconteça e, caso aconteça, que o impacto seja o menor possível, ainda que a ameaça não seja conhecida e que as soluções de segurança não consigam identificá-la no primeiro momento.

(\*) É diretor de serviços de segurança da McAfee para a América Latina.

## Looke abre quatro vagas para área de desenvolvimento

Looke, plataforma brasileira de streaming de vídeos on demand, está com quatro vagas abertas para desenvolvedores na cidade de São Paulo - SP. Dentre elas, duas são: Programador Sênior .Net C# para Windows 10 e Programador Pleno .Net C# para orientação a objetos de arquitetura MVC 4 e 5 Razor.

Para as plataformas mobile, existe 01 vaga para Programador Sênior IOS e 01 vaga para Programador Sênior Android. Os currículos devem ser enviados para o e-mail: vagas@looke.com.br até o dia 18 de agosto de 2017.

Conhecimento necessário: Programador Sênior .Net C# em Windows 10 - é necessário conhecimento em .Net para Xbox 360 e One, JavaScript MVC Framework (Knockout, Angular, Ember ou similar),

Threads, Delegates, WPF, WCF, TDD, NUnit, Orientação a objetos, Arquitetura MVC 4 e 5 Razor, .Net 3.5, .Net 4 e .Net 4.5, ADO.NET Entity, Linq, Lambda, Scrum, Kanban, MS SQL Server, Ajax, JQuery, JSON, CSS, HTML5 e Inglês fluente.

Programador Pleno .Net C# em Orientação a objetos - capacidade de uso em arquitetura MVC 4 e 5 Razor, .Net 3.5, .Net 4 e .Net 4.5, ADO.NET Entity, Linq, Lambda, Scrum, Kanban, Bancos de dados SQL Server, JavaScript, Ajax, JQuery, JSON, JS, HTML5, CSS, Aplicativos Facebook e Inglês intermediário/avançado.

Vagas mobile IOS Xamarim/UWP - experiência de, no mínimo, 03 anos com a linguagem nativa de cada plataforma e conhecimentos avançados de C++. Inglês Intermediário/avançado.

## News @TI

### SND fecha parceria de distribuição com a HP

A SND, uma das principais distribuidoras de produtos de tecnologia do Brasil, anuncia acordo para a distribuição oficial das linhas de notebooks, desktops, impressoras e suprimentos da HP no país. A expectativa é de que a parceria represente um crescimento de aproximadamente 10% no faturamento da distribuidora já para este ano (atendimento.hp@snd.com.br).

### Brasileira MC1 se estabelece como principal fornecedora de soluções digitais na AL

A MC1 - multinacional brasileira, com foco em processos, utilizando a mobilidade como ferramenta para negócios inteligentes e entregando maior produtividade para equipes internas e externas - passa por um momento positivo de transformação. Com o aporte recebido recentemente da G5 Evercore e da co-investidora Cassis, a empresa turbinou a sua solução Win The Market, contratou novos executivos, concretizou importantes negócios e torna-se, globalmente, um dos maiores players digitais para as áreas de execução da força de vendas, merchandising e utilities. Reconhecida pelo Gartner no "Market Guide for Retail Execution and Monitoring Solutions for the Consumer Goods Industry" como líder na América Latina, a MC1 tem expectativa de dobrar o seu número de usuários Cloud até 2018.

# Seis dicas valiosas para um webinar de sucesso

Despertar a curiosidade e obter engajamento são algumas dicas da detentora da ferramenta GoToWebinar, LogMeIn

pela facilidade, agilidade e economia de tempo e dinheiro, fazer palestras e workshops virtuais está cada vez mais comum no Brasil. Antes, para fazer uma palestra tradicional era necessário arcar com itens como aluguel de sala, sistema multimídia, alimentação e até estacionamento. Agora basta um palestrante, uma boa ferramenta de webinar e algumas dicas preciosas para que seu próximo evento virtual seja um sucesso. Os webinars estão se tornando, sem dúvida, uma das atividades de marketing mais poderosas para conquistar clientes. Eles oferecem uma oportunidade única para geração de leads, clientes potenciais, e de reunir dados em tempo real sobre o público alvo.

"Acredito na capacidade de conversão dos webinars nas mais diversas etapas da jornada de um cliente. Desde a percepção da marca, geração de leads, aquisição de clientes até a retenção e lealdade dos mesmos, os webinars oferecem uma maneira poderosa de mover as pessoas para uma ação desejada", ressalta Gustavo Boyde, Head of Marketing da LogMeIn para a América Latina.

Em uma pesquisa da LogMeIn 70% dos profissionais de marketing classificaram que os webinars são efetivos ou muito efetivos na geração de leads qualificados. Se tornando assim uma parte importante do mix de marketing. Com o uso de uma solução adequada, como o GoToWebinar, organizar um evento online se tornou relativamente simples. As ferramentas ajudam desde a divulgação dos eventos até as campanhas de marketing posteriores ao evento.

Gustavo Boyde dá algumas dicas de como realizar um webinar de sucesso utilizando a ferramenta. Confira:

### 1. Desperte a curiosidade

Um estudo do site MarketingProfs concluiu que promover um webinar por mais de 7 dias pode aumentar o tamanho da audiência em até 36%, o indicado seria de 4 a 6 semanas, mesmo que a maioria dos participantes se inscreva nos últimos dias. Porém, tão importante quanto divulgar com antecedência é promover o evento nas últimas horas, enviando um e-mail final como lembrete com 24 horas de antecedência se mostrou bastante efetivo. Utilize a função para o envio de e-mails automáticos em diferentes datas, desperte curiosidade e interesse nas comunicações ao invés de enviar apenas detalhes. Vale ressaltar que você deve buscar atingir o seu público em potencial pelo menos três vezes.

### 2. Facilite a inscrição

O seu objetivo neste momento é se aproximar de uma nova audiência. Tome cuidado para não parecer intrusivo e solicitar uma quantidade muito grande de informações para o registro no webinar, criando assim uma barreira para os participantes. Você pode customizar o formulário de inscrição para solicitar apenas informações básicas de identificação do lead e, a partir daí, usar pesquisas e análises posteriores para capturar mais informações dos interessados.

### 3. Abuse das interações em tempo real

Assistir um evento ao vivo é muito mais eficaz do que ler artigos e por isso muitas pessoas adoram participar de webinar sobre seus assuntos de interesse. Explore os recursos de levantar a



## Como os ciberataques estimulam o mercado de profissionais de segurança da informação?

Equipamentos e sistemas continuam, em sua grande parte, sendo operados por seres humanos e, invariavelmente, são suscetíveis a erros. De acordo com dados da Pesquisa Global de Segurança da Informação 2016 promovida pela PwC, 41% dos entrevistados informaram que os incidentes de segurança da informação nas empresas envolveram os funcionários. O estudo ouviu 600 empresas sediadas no Brasil. Entre os principais incidentes relatados estão o roubo de propriedade intelectual e dados de clientes, com impacto direto nos recursos financeiros das corporações.

Trinar colaboradores para operar sistemas computacionais pode minimizar incidentes associados a segurança da informação. Contudo, esta iniciativa caracteriza apenas um dos pontos que devem ser levados em consideração para o aprimoramento da segurança nas empresas. Além do investimento em tecnologia e treinamento dos colaboradores, é de suma importância que os times de segurança estejam alinhados aos conceitos associados a defesa eletrônica e/ou cibernética. Estes dois segmentos estarão entre as principais profissões do futuro. No Brasil, institutos universitários já se mobilizam para abrir cursos e formar tecnólogos com tais competências.

Por sua dimensão, número de habitantes e posicionamento, nosso país está sob a mira de potenciais atividades maliciosas, o que requer a necessidade de estarmos à frente no que diz respeito a profissionalização de especialistas no segmento. De acordo com informações publicadas no estudo Networking Skills, divulgado pela Cisco em parceria com a IDC, a estimativa é que até 2019 haja uma demanda no mercado de 46% por profissionais de rede para atuar na América Latina. Isto inclui aqueles



cujo foco de atuação seja a segurança da informação.

A pesquisa vem de encontro a outra que cabe ser citada, organizada pelo Banco Interamericano de Desenvolvimento (BID) e pela Organização dos Estados Americanos (OEA), divulgada neste ano. A América Latina se torna um alvo fácil para a ação de cibercriminosos por concentrar um alto uso de dispositivos com Windows nativo, além da não preocupação em manter os sistemas atualizados. Tanto que o Brasil foi um dos vinte

países mais atingidos - o único da América Latina, neste grupo - quando da ocorrência do ciberataque envolvendo o ransomware WannaCry em maio passado.

Com o crescimento da necessidade desse tipo de perfil profissional, em virtude, sobretudo, dos ciberataques, aumenta também a expectativa salarial. Estima-se que a média dos salários de profissionais que atuam nesse segmento varia entre cerca de R\$ 5.800, em 2016, até R\$ 11.500, em 2017, considerando níveis hierárquicos e suas obrigações. Ou seja, a possibilidade de renda superior também potencializa o interesse pelo segmento, elevando a oferta de especializações na área.

Cursos sobre criptografia, testes de invasão de redes, análise de vulnerabilidade em redes/software e análise forense de redes são algumas das capacitações promovidas por empresas e entidades especializadas em segurança da informação, no Brasil e no exterior. Seguramente, profissionais que já atuam no segmento de tecnologia e desejam se especializar em segurança digital, investindo em especializações desse nível, estarão na vanguarda do conhecimento.

(Fonte: Cassio Brodbeck, CEO da OSTE Business Security, especializada em segurança virtual corporativa).