



KES

Knowledge Exchange Sessions

DUDU MIMRAN

CTO DO TELEKOM INNOVATION LABORATORIES
EM ISRAEL

INVISIBLE FORCES: CYBER SECURITY, AI AND BLOCKCHAIN

A CIBERSEGURANÇA VEIO PARA FICAR

COM O AUMENTO DA CONECTIVIDADE EM REDE, NAS DUAS ÚLTIMAS DÉCADAS A NECESSIDADE DE AS EMPRESAS INVESTIREM EM CIBERSEGURANÇA VIROU ALGO CENTRAL E FATOR CRÍTICO.

Só no ano passado foram contabilizados 27 bilhões de dispositivos conectados e em média ocorrem 12 trilhões de tentativas de ataques por dia, segundo dados da empresa de segurança Norse. Os ataques cibernéticos se multiplicam na mesma velocidade que os equipamentos conectados.

“A cibersegurança veio para ficar, e vai se tornar uma espécie de indústria de saúde para máquinas”. Foi assim que o israelense Dudu Mimran alertou os participantes do **KES (Knowledge Exchange Session)**, realizado no dia 25 de abril. Com a experiência de quem trabalha com cyber security desde os anos 80, ele apresentou um panorama sobre as ameaças virtuais, o crescimento desse mercado, o que o futuro nos reserva e quais medidas devemos tomar para não comprometer nossos negócios.





Até o fim da década de 90, as ameaças eram bem mais simples. Geralmente, explicou Mimran, analisava-se a assinatura de um vírus, descobria-se um padrão e esse padrão era replicado nos softwares antivírus. A ação era o suficiente para coibir a maioria dos ataques. Mas o mundo mudou de lá pra cá e os ataques ficaram bem mais complexos.

A mudança nesse cenário se deu recentemente -- mais precisamente em 2013. Nessa época foram criados os ataques polimórficos — que consistem na criação de variações de um vírus. Na prática, isso fez com que algumas pragas passassem incólumes por programas antivírus, facilitando a vida de cibercriminosos. ***“Por essa razão é que temos toda a indústria de cibersegurança. Os hackers criaram um nível de complexidade e sofisticação que os defensores não estavam conseguindo lidar”,*** afirmou.

Segundo dados da CB Insights, o mercado de cibersegurança nunca esteve tão quente, com um investimento de US\$ 6 bilhões em investimentos na área em 2017. Só no 1º semestre do ano passado, seis startups do ramo levantaram mais de US\$ 100 milhões. Portanto, a indústria do “cuidado com as máquinas” está em alta.

QUEM ATACA?

Os agentes que atacam são diversos. Podem ser feitos por estados, grupos terroristas, crime organizado, hackers ativistas, insiders ou simplesmente hackers. As motivações também variam muito: espionagem, dinheiro, ideologia ou senso de injustiça.

O negócio de burlar a segurança digital reúne uma série de características que o torna atrativo. Sempre é algo reativo (as empresas esperam acontecer para tomar uma atitude), é lucrativo, é fácil de trabalhar (quem ataca cada vez mais compartilha suas ferramentas entre si) e costuma ser muito difícil achar o responsável.

Existe ainda uma outra vantagem que beneficia o hacker. Enquanto o responsável pela segurança de uma empresa precisa estar atento a qualquer ponto vulnerável, para o cibercriminoso basta focar em um ponto fraco e estudá-lo com profundidade. Muitas vezes a ferramenta mais poderosa de um hacker é a engenharia social. ***“Se quero hackear um banco, por exemplo, posso criar um ataque contra a secretária do CEO, que tem acesso ao computador dele”***, explicou Mimran.



O QUE VEM POR AÍ?

Atualmente, boa parte dos ataques é feito por pessoas, na maioria das vezes usando bots (máquinas infectadas controladas por um cibercriminoso). Porém, estamos cada vez mais próximos de uma nova onda de ataques, quando entra em cena a inteligência artificial. ***“Ciberataques vão ser mais rápidos, adaptáveis e terão grande escala. Eles serão mais baratos e muito sofisticados, fazendo com que vários serviços sejam derrubados.”***

Para ele, já em 2018 devemos ter uma primeira evolução desse tipo de ataque. Ainda que toda a discussão sobre inteligência artificial seja catastrófica, do tipo ***“quando as máquinas vão nos destruir?”***, Mimram acredita que humanos usando inteligência artificial são ainda mais perigosos que criações de inteligência artificial feitas por ela própria. De qualquer jeito, essa terceira onda terá grande impacto e vai derrubar, literalmente, várias operações digitais.





Apesar disso, Dudu é otimista em relação ao futuro. Ele acha que as empresas vão usar inteligência artificial para contra-atacar, mas ainda vão bater cabeça sobre esse assunto. Segundo ele, a origem de muitos problemas relacionados a segurança vem do fato de a tecnologia não ser desenvolvida para ser segura, e sim para funcionar.

“Um exemplo de tecnologia segura é blockchain. Com uso de criptografia e por ser um banco de dados distribuído imutável, ela faz até com que estranhos confiem na aplicação”, explicou.

A inteligência artificial pode ser usada ainda para detectar ameaças. Os humanos costumam ser ineficientes para resolver problemas. Já as máquinas podem antecipar o risco e evitar um problema.

COMO TENTAR SE PREVENIR

Os desafios na área de segurança são grandes e, após 25 anos de experiência, Dudu Mimran listou como empresas podem se estruturar para ter uma postura mais proativa nos cuidados com cibersegurança:

1. COLABORAÇÃO

É necessário que haja algum tipo de colaboração da indústria no compartilhamento de inteligência. “A tendência das empresas é cada uma ficar na sua, mas todas elas são alvos de ataques recorrentes”, afirmou.

2. GASTOS SEGURANÇA X TECNOLOGIA

É preciso entender o nível de investimento de segurança e do nível de investimento em tecnologia da informação. Essa correlação pode dizer muito sobre o tipo de prioridade que sua empresa tem.

3. CUIDADO COM SEGURANÇA FÍSICA E DIGITAL

O responsável pela segurança deve também gerir instalações físicas e digitais. Isso faz sentido, pois os ataques são feitos das duas formas.

4. TECNOLOGIA E SEGURANÇA DEVEM ESTAR JUNTOS

O pessoal da tecnologia sempre quer implementar novos produtos, mas a segurança geralmente impede. Logo, esses dois setores, ainda que conflitantes, devem trabalhar juntos para evitar maiores problemas.



Q&A

Logo após a palestra, participantes fizeram perguntas ao convidado. Rafael Hawilla, Diretor Geral do Boa Vista, questionou sobre a iminência de uma ciberguerra. Mimran disse que o risco existe, pois cada vez mais dependemos da tecnologia e isso nos torna vulneráveis.

“Máquinas fazem comida, remédio e conduzem veículos autônomos. Se as máquinas forem atacadas, nós teremos algum tipo de consequência.”

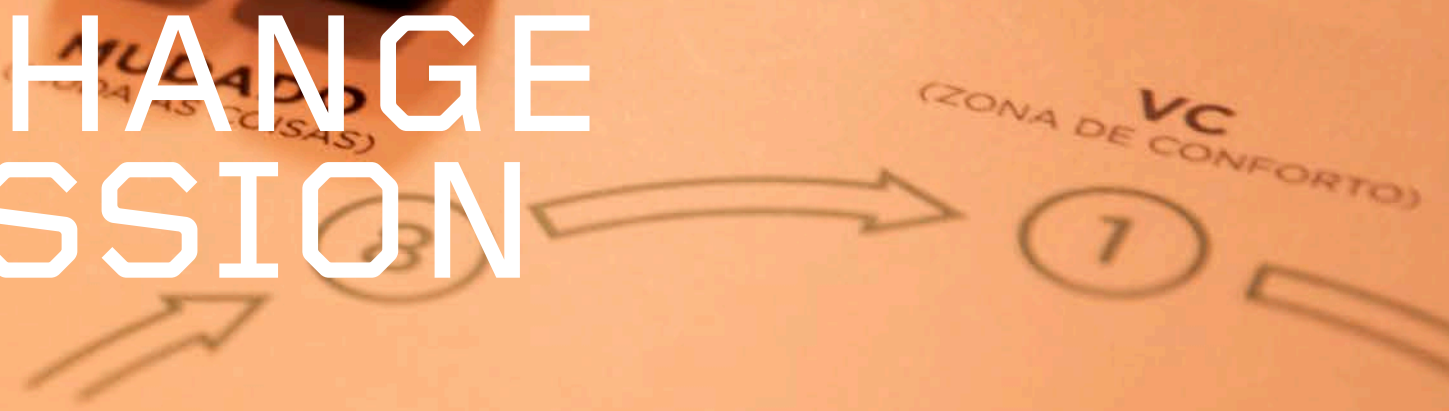
Sérgio Herz, CEO da Livraria Cultura, perguntou sobre blockchain e como ela deve influenciar a indústria. Sobre isso, o especialista disse que pode ser revolucionário para finanças e em qualquer tipo de interação entre estranhos.

Já Rafael Bastos, do Itaú, perguntou sobre os serviços na nuvem de grandes plataformas, como os oferecidos por Amazon, Microsoft e Google, e quais as preocupações de segurança que as companhias devem ter. “Pense em uma fábrica e se eu colocar todos os dados dela na nuvem. Pode haver um grande risco para o negócio no caso de uma invasão”, disse Dudu.

EXCHANGE SESSION



SMK SMK SMK



O MUNDO DA CIBERSEGURANÇA DESPERTA FASCÍNIO E CURIOSIDADE. NÃO É À TOA QUE O TEMA ESTÁ PRESENTE EM FILMES E SÉRIES. POR ESSA RAZÃO, A SESSÃO DE TROCA DE CONHECIMENTO DESSA EDIÇÃO DO KES CONTOU COM UMA AJUDA DE JOTAGÁ CREMA, O ROTEIRISTA E DIRETOR DA SÉRIE 3% DA NETFLIX.

CREMA EXPLICOU COMO CONSTRUIR UM ROTEIRO E, A PARTIR DISSO, OS PARTICIPANTES TINHAM A MISSÃO DE CRIAR UMA HISTÓRIA EM 15 MINUTOS, BASEADA EM ALGUNS CENÁRIOS E PERSONAGENS FICTÍCIOS. NO FINAL DA DINÂMICA, CREMA AVALIOU O ROTEIRO, ENQUANTO DUDU FALOU SOBRE SEGURANÇA E AS IDEIAS QUE FAZEM SENTIDO NO MUNDO REAL.



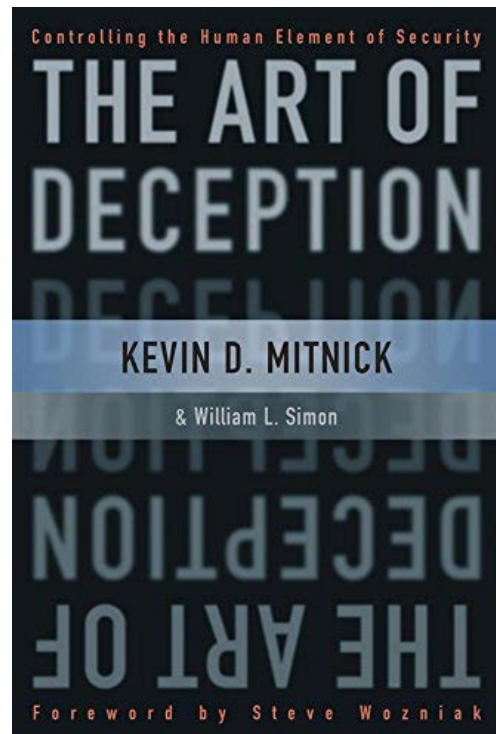
O grupo de **Marcelo Câmara**, do Bradesco, teve como personagem Henrique, um filantropo, fundador de ONG e herdeiro pressionado a assumir os negócios da família. Mesmo contrariado, o personagem assume a companhia após a morte dos pais e começa a atacar seus antigos amigos, que o acusavam de ser traidor. Ele contrata hackers, derrota os antigos amigos e, no fim, vê que se tornou como seu pai.

Já o grupo de **Vanessa Fonseca**, da Accenture, bolou uma história em que João, CEO e surfista, está planejando uma viagem e concede uma entrevista na TV. Isso causa inveja em Pedro, profissional de T.I. Ele então faz um plano para roubar dinheiro de João. Para isso, usa engenharia social para invadir o computador da secretária dele, hackeia o e-mail de João e pede para a funcionária fazer uma transferência de dinheiro.

“Pode acontecer”, disse Mimran. “A parte de engenharia social é comum, mas teria forma mais fáceis de interceptar a comunicação. Tem um aparelho que poderia forçar um celular a se conectar a uma rede falsa de telefonia. No geral, isso não é ficção científica. Está acontecendo.”

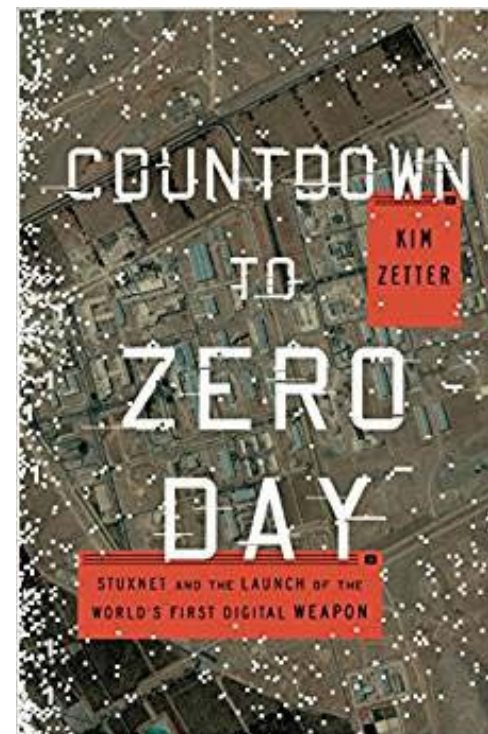


PARA SE APROFUNDAR NO TEMA E ENTENDER COMO VOCÊ E SUA EMPRESA PODEM SE PROTEGER DE CIBERATAQUES, AQUI ESTÃO OS LIVROS INDICADOS POR DUDU MIMRAN:



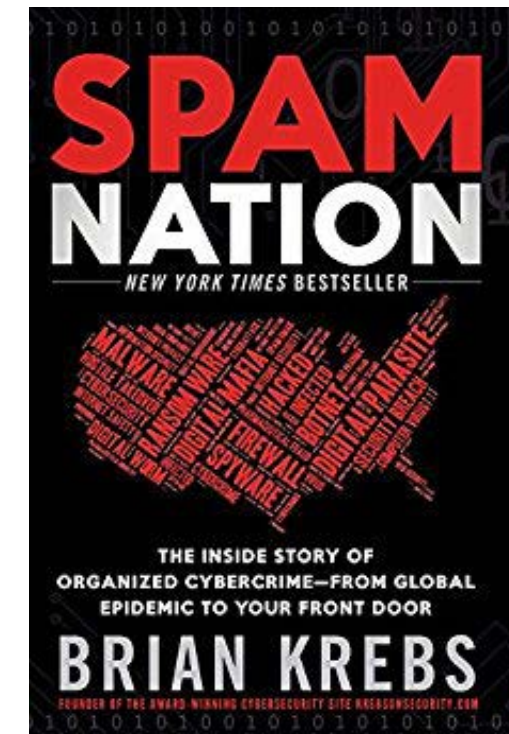
**The Art of Deception:
Controlling the Human
Element of Security
(Kevin Mitnick)**

Mostra como cibercriminosos manipulam humanos para realizar ataques.



**Countdown to Zero Day:
Stuxnet and the Launch of the
World's First Digital Weapon
(Kim Zetter)**

Conta a história por trás do vírus que sabotou os esforços nucleares do Irã.



**Spam Nation: The Inside Story
of Organized Cybercrime—from
Global Epidemic to Your Front
Door (Brian Krebs)**

Revela como funciona a economia do spam e as mentes por trás desses golpes.

INSPIRED BY:

Accenture Interactive

Oath:
A Verizon company

Knowledge Exchange Sessions

WWW.KES.DO

INSTAGRAM

TWITTER

FACEBOOK

G+

LINKEDIN