COMPUTERWORLD

PREPARAR OS TRABALHADORES PARA A CIBERSEGURANÇA

COMPUTERWORLD **www.computerworld.com.pt**

Av. da República, N.º 6, 7º Esq. 1050-191 Lisboa
Director Editorial: **João Paulo Nóbrega** jnobrega@computerworld.com.pt
Redactora: **Mafalda Simões Monteiro** mmonteiro@computerworld.com.pt
Director Comercial: **Paulo Fernandes** pfernandes@computerworld.com.pt
Telef. / Fax +351 213 303 791

IDG

A IDG (International Data Group) é o líder mundial em media, estudos de mercado e eventos na área das tecnologias de informação (TI). Fundada em 1964, a IDG possui mais de 12.000 funcionários em todo o mundo. As marcas IDG - Computerworld, CIO, CFO World, CSO, ChannelWorld, InfoWorld, Macworld, PC World e TechWorld - atingem uma audiência de 270 milhões de consumidores de tecnologia em mais de 90 países, os quais representam 95% dos gastos mundiais em TI. A rede global de media da IDG inclui mais de 460 websites e 200 publicações impressas, nos segmentos das tecnologias de neg cio, de consumo, entretenimento digital e videojogos. Anualmente, a IDG produz mais de 700 eventos e conferências sobre as mais diversas áreas tecnol gicas. Pode encontrar mais informações do grupo IDG em www.idg.com

COMO FORMAR OS RECURSOS HUMANOS?

Todas as empresas procuram a resposta para esta pergunta. Ou deviam fazê-lo. Afinal, quando o elo mais fraco da cibersegurança é frequentemente o utilizador final, todas as acções preventivas são essenciais, a começar pela formação.

Ao mesmo tempo que ataquAo mesmo tempo que ataques mais mediáticos como o ransomware Wanna Cry servem de alerta, surgem novas ameaças diariamente, como os malwares Petya e Bad Rabbit. São ataques cada vez mais sofisticados, mas o factor humano nem sempre ajuda na defesa, antes pelo contrário.

Os utilizadores comuns, e os seus dispositivos, são muitas vezes a porta de entrada para os sistemas da sua empresa (46% das vezes, segundo a Kaspersky).

"Em última análise, todos os funcionários de uma organização têm de compreender que a segurança dos sistemas de informação da empresa começa e termina neles próprios", alerta Sandra Joaquim, directora de vendas da área de Formação da Olisipo, empresa que trouxe para Portugal formações e certificações CyberSafe em 2016.

E os avisos devem ser feitos com regularidade. "Uma regra de ouro é que a sensibilização de todos os colaboradores deve ser feita periodicamente e não uma única vez e nunca mais se falar no assunto", diz Cláudia Vicente, directora da Galileu.

Esta sensibilização deve ser feita no âmbito de um plano de consciencialização para a segurança que depende de vários factores. "Como cada caso é específico, o plano irá depender das características do negócio, do tipo de empresa, da dispersão (uma única localização ou várias localizações), do tipo de colaboradores, do tipo de conhecimento desses colaboradores, entre outros factores", assinala a responsável da Galileu. A empresa já tem mais de 50 cursos na área da segurança informática, incluindo cursos de certificação EC Council, Cisco, Microsoft, entre outros.

Claudia Vicente, directora da Galileu

De facto, o "descuido dos colaboradores é uma das maiores falhas de cibersegurança no que diz respeito a ataques direccionados", diz a Kaspersky. Além da falta de literacia tecnológica e de recursos qualificados,

Sandra Joaquim, directora de vendas da área de Formação da Olisipo

entre os maiores desafios que as empresas enfrentam actualmente estão as técnicas de "engenharia social", incluindo as de "phishing".

Desafio da engenharia social

Os esquemas de engenharia soOs esquemas de engenharia social consistem num foco de ameaça e são destacados por Pedro Veiga, coordenador do Centro Nacional de Cibersegurança (CNCS). Apesar de não estar de acordo com o termo que se convencionou chamar: "engenharia social", Pedro Veiga explica que "as pessoas recebem telefonemas ou mensagem que as levam a disponibilizar as suas credenciais e dados de acesso que, posteriormente são usados para acções de fraude". É importante que as pessoas estejam alerta e que, nas organizações, exista quem as apoie a um nível mais técnico.

"E-mails de phishing, palavras-passe fracas, chamadas falsas de equipas de apoio técnico. Já vimos de tudo. Mesmo um cartão de memória caído no parque de estacionamento ou próximo de uma secretária pode comprometer toda a rede (…) e originar o caos", recorda David Jacoby, investigador de segurança na Kaspersky Lab.

Aposta na formação

A tecnologia não é a solução para uma protecção completa. Sandra Joaquim, da Olisipo, considera que o "segredo está no equilíbrio entre a tecnologia, a formação e a cultura corporativa para contornar os problemas e minimizar as ameaças". A responsável recorda o célebre ataque à cadeia de lojas norte-americana Target, em 2013. "O software anti-intrusão deu alertas inúmeras vezes, no entanto não houve qualquer resposta humana. O resultado foi o roubo de 100 milhões de dados pessoais".

O plano [de sensibilização] irá depender das características do negócio, do tipo de empresa, da forma como existe (uma única localização, ou dispersa por várias localizações), do tipo de colaboradores, do tipo de conhecimento desses colaboradores, entre outros factores", assinala Cláudia Vicente, directora da Galileu.

Sandra Joaquim explica que a maior causa dos incidentes [de cibersegurança] é ainda a

Pedro Veiga recomenda

- Nunca abrir mensagens de correio electrónico de origem desconhecida, pois pode transportar consigo malware;
- Fazer cópias de segurança periódicas (backups);
- Manter os sistemas e as aplicações actualizados;
- Ser cauteloso ao clicar em endereços (links) incluindo em mensagens de correio electrónico provenientes de endereços conhecidos, uma vez que as técnicas para forjar emails têm vindo a evoluir;
- Configurar servidores de email correctamente.

falta de formação e consciencialização, que permite que as ameaças se tornem incidentes. Exemplificando, basta uma "pen" não autorizada entrar num sistema crítico e todos os esforços de segurança podem ficar comprometidos".

E o problema não está necessariamente no custo da formação. "O investimento na formação para não-técnicos é ainda extremamente acessível. Mesmo quando falamos de formação certificada, o valor acrescentado é muito alto comparativamente ao investimento", explica a responsável da Olisipo.

Na mesma linha, também Alfonso Ramírez, director-geral da Kaspersky Lab Ibéria, considera que a ciberprotecção não reside apenas no patamar da tecnologia, "mas também na cultura e treino da organização". Para o alcançar, a cultura de cibersegurança deve ser positiva, "baseada numa abordagem educativa em vez de restritiva, do topo para as bases". Desse modo, os resultados serão óbvios", assinala.

Além da "segurança reactiva perante os incidentes", as empresas precisam de promover "uma segurança pró-activa quando elaboram uma estratégia de segurança", onde se inclui, naturalmente, o "investimento na formação dos colaboradores" quanto a "conceitos básicos sobre cibersegurança", assinala Ramirez. ■

Rui Duro, director de Vendas para Portugal da Check Point

Recomendações para melhorar o comportamento dos utilizadores

• Os utilizadores devem ser conscienciali-zados para um conjunto de perigos e fraudes das quais podem ser vítimas e, consequentemente, tomar medidas para se protegerem das mesmas (Kaspersky Lab)

• Criar uma política de segurança da empresa que obrigue todos os utilizadores a se comprometerem com ela. Entre outras coisas, informar e avisar os utilizadores da empresa que os sistemas são de utilização profissional e não pessoal (Check Point)

• Os utilizadores devem utilizar software de segurança nos seus dispositivos, assegurar que instala as actualizações de segurança no seu sistema operativo assim que estas estiverem disponíveis e certificar-se que navega em websites que tenham o certificado de segurança 'HTTPS' – onde o S significa Seguro (Kaspersky Lab)

• As empresas devem investir equilibradamente na formação de colaboradores técnicos e não técnicos, porque o "castelo" protege-se em todas as frentes. É impossível colocar toda a responsabilidade num departamento técnico, quando o resto da empresa é uma constante ameaça interna à segurança da informação (Olisipo)

• Fazer permanentemente acções de sensibilização sobre riscos, os comportamentos, e ataques específicos que possam surgir (Check Point)

• Para uma navegação segura na Internet, os utilizadores devem seguir as seguintes recomendações: "não aceder a sites que desconhecem"; "não clicar em links para aceder a sites"; "não armazenar credenciais (passwords) localmente" e se vão aceder ou partilhar informação privada façam-no apenas se o endereço (URL) indicar https:// e nunca http://" (Galileu/Rumos)

• A Check Point recomenda que, dentro das empresas, se criem "equipas próprias para a segurança, que olhem a segurança como um todo e não apenas como tecnologia". Para Rui Duro estas pessoas devem "ter poder e capacidade para tomar decisões que, por vezes, poderão não ser muito populares".

• Na Cisco a equipa de TI promove uma componente formativa junto dos colaboradores. Pode, por exemplo, enviar simulações de spam. Caso o colaborador clique num determinado link é remetido para uma página da empresa na qual se explica porque não deveria ter clicado, detalhou Rui Brás Fernandes, gestor de engenharia de sistemas na Cisco Portugal. ▪

Habilitar o país para a cibersegurança

Para fazer face à falta de recursos humanos formados para a cibersegurança, qualitativa e quantitativamente, o CNCS está a trabalhar em múltiplas frentes.

Um dos objectivos do Centro Nacional de Cibersegurança (CNCS) é a promoção da formação dos utilizadores em cibersegurança. Para o efeito, o CNCS organizou em Junho uma conferência nacional sobre o tema (C-Days) que reuniu várias centenas de responsáveis da Administração Pública e de outros organismos para debater o Estado da Nação. Mas esta é apenas uma das iniciativas deste braço da Autoridade Nacional de Segurança (ANS), cuja missão abarca todas as dimensões da segurança, incluindo a cibersegurança.

Nesta fase, o CNCS está a concentrar as suas atenções na Administração Pública tendo promovido, em 2017, várias edições do "Curso Geral de Cibersegurança", um pouco por todo o país.

Neste âmbito têm sido igualmente promovidas as acções "cibertemas", nas quais é promovida a cibersegurança junto dos cidadãos, empresas e entidades públicas, e que teve um dos seus pontos altos em Outubro, no âmbito do Mês Europeu da Cibersegurança, coordenado pela Agência Europeia para a Segurança das Redes e da Informação (ENISA). Foram debatidos temas como o Regulamento Geral de Protecção de Dados e a Directiva de Segurança das Redes e da Informação.

Pedro Veiga, coordenador do CNCS, explica que o objectivo é "implementar boas práticas na área de cibersegurança", tanto em gestores de topo como em utilizadores finais.

Para contribuir para o combate ao desemprego, o centro está também a desenvolver, em parceria com a Segurança Social, sessões de formação, enquanto trabalha "em muitas outras iniciativas", dirigidas a "entidades específicas".

Plataforma aberta ao grande público

Para chegar a todos, o CNCS está a criar uma plataforma aberta, dirigida ao grande público, em parceria com empresas privadas, que darão também acesso a boas práticas de cibersegurança. Esta plataforma irá incluir conteúdos produzidos pelo CNCS, como é o caso de um vídeo protagonizado pelo coordenador do centro, mas também contará com contributos externos.

Também a Cisco quer contribuir para que "a Administração Pública, as empresas e as pessoas, enquanto indivíduos, se protejam online", disse Rui Brás Fernandes, gestor de engenharia de sistemas na Cisco. A empresa já disponibilizou, online e gratuitamente, o "curso de iniciação à cibersegurança" que pretende explicar como se pode uma pessoa "proteger online, nos media sociais, enquanto procura oportunidades de emprego", etc. Este curso faz parte integrante do programa Networking Academy da Cisco. Neste momento, "a empresa está a trabalhar com várias entidades públicas e privadas com o objectivo de disponibilizar estes cursos como base de formação à cibersegurança em outras entidades", disse António Feijão, director-geral de IoT na Cisco Portugal. ■

Pedro Veiga, coordenador do Centro Nacional de Cibersegurança (CNCS)

"Há falta de visão sistémica"

A cibersegurança "é uma questão de interesse nacional" que não está ainda no topo das preocupações da governação das organizações, afirma José Tribolet, coordenador da Leadership Graduate Academy, do IST.

O curso de cibersegurança da Leadership Graduate Academy, do Instituto Superior Técnico (IST) continua "em banho-maria". José Tribolet, coordenador da academia, explica que as empresas precisam e querem recursos, mas não estão dispostas a abrir os cordões à bolsa ou a colocar os seus colaboradores em formação intensiva durante seis meses. No entanto, a cibersegurança "é uma questão de interesse nacional" que só está a ser acautelada pela "governance" de organizações militares ou ligadas à segurança nacional.

Fazendo a analogia à estrutura militar, José Tribolet, coordenador da academia, assinala que, salvo as organizações militares e análogas que têm um "Estado-Maior" alerta e estratégias de "governance", a maioria das organizações não tem "o trabalho de casa" feito. Para além do Estado-Maior falta-lhes ainda líderes e operacionais.

Para avançar com a nova "fábrica de reconversão de servidores de carbono (pessoas)", o responsável procura criar parcerias com o mercado que lhe forneça matéria-prima para desenvolver recursos, que no final irão para as empresas. Pelo meio esses parceiros terão de colocar os quadros em formação intensiva, mas mantendo-lhes as condições para continuarem a viver.

O arranque da primeira edição tem vindo a ser adiada desde o início de 2017. Esta situação é exemplo da falta de visão sistémica que o País atravessa, diz Tribolet.

Computerworld - Os líderes das organizações portuguesas estão sensibilizados para as questões da cibersegurança?

José Tribolet - Impressiona-me que não exista um fórum para debater o tema da cibersegurança ao nível intelectual na Administração Pública. Penso que, antes de comprar soluções a grandes multinacionais é necessário pensar, perceber e interiorizar ideias. O debate existe, mas é condicionado pelas forças comerciais, que, não sendo mau, apresentam visões parciais. Não existe uma visão sistémica. Os responsáveis máximos da maior parte das organizações não têm formação de base para entender o que se está a falar.

CW - Não há excepções?

JT - No sector militar, em matéria de cibersegurança e ciberdefesa existe um nível de topo em governação, graças sobretudo à NATO. As Forças Armadas também têm gente e cursos. Mas apesar de termos o Estado-Maior todo e os assessores jurídicos, mas não temos forças de combate. Não temos soldados nem comandantes de tropas em combate. E isto é dramático.

CW - Quais as suas propostas para mudar essa "status quo"?

JT - Antes de mais, o CIO deveria ser uma pessoa preocupada com a informação e com a segurança da informação e não apenas com a tecnologia. Para o efeito o Instituto Superior Técnico (IST) está a renovar a sua oferta de formação adaptando-se ao cenário de transformação digital generalizada.

O IST opera em três vectores clássicos - formação de grau

José Tribolet, coordenador da Leadership Graduate Academy

académico de base, I&D e empreendedorismo. Agora está a ser desenvolvido um novo vector com a missão de conferir capacidades às pessoas não ao nível de base, mas ao longo da vida, a que gosto de chamar "update" do sistema operativo e das aplicações do 'servidor de carbono', as pessoas.

CW - Que na prática significa…

JT - Há uma lacuna enorme de recursos humanos nestas áreas [de cibersegurança] em todo o mundo, na Europa e em Portugal. Na minha opinião esta lacuna é talvez o maior impedimento à criação de riqueza no nosso País nos próximos anos. É necessário fazer acções decisivas de reconfiguração, de reconversão de muita gente que têm empregos de menor valia ou estão mesmo desempregados, para que se lancem em carreiras de valor acrescentado.

A nossa formação é dura. Implica capacidade individual e colectiva de saber identificar um conjunto de problemas que afligem uma determinada situação para em seguida agir no sentido de resolver alguns problemas e aprendendo.

CW - CW - Qual é a oferta para a formação de quadros profissionais?

JT - No Técnico, existe uma grande linha, já histórica, promovida pela Associação para a Formação e o Desenvolvimento em Engenharia Civil e Arquitectura (FUNDEC) vocacionada para aqueles quadros, em que se promovem cursos de especialização, curtos, muito bem definidas, sobre novas tecnologias, no- vos métodos, novas máquinas, novos materiais, etc.

Na área da Engenharia informática temos, desde 1999, o POSI, que começou por ser a Pós-Graduação em Sistemas de Informação e que tem evo luído até ao modelo actual: Mastering Enterprise Engineering for Digital Transformation.

Em 2015, lançámos a Pós-graduação em Engenharia de Software e dos Sistemas de Informação Empresariais (SISe), a nossa primeira fábrica de reconfiguração de servidores de carbono. É um curso intensivo, de seis meses que visa qualificar e dar capacidades efectivas de saber fazer no domínio da engenharia de software e sistemas de informação empresariais com requisitos de partida bastante elevado.

A SISe foi criada a pedido da Deloitte e já atribuiu diplomas de formação avançada (3º ciclo de Bolonha) a mais de uma centena de profissionais. A quarta edição começa em Fevereiro de 2018.

Os alunos entram às 9h00 saem oficialmente às seis ou sete. São seis meses no duro. E só assim é que funciona. Penso que o vínculo contratual é muito importante. Têm um patrão, é isso que tem de fazer, tem um horário. São profissionais disto. Só fazem isto.

CW - E há também o curso na área da cibersegurança…

JT - Esse é um curso que permite ter uma visão da segurança da informação, das redes, dos sistemas operativos, das máquinas, das aplicações, da segurança física, da segurança organizacional. É uma visão 360º da segurança. Depois, no terreno vão ganhar competências e especializações. Não são propriamente soldados, ao Técnico compete-nos fazer capitães de combate.

Começou a ser desenhado em 2016, está aprovado e legislado. Visa formar pessoas em cibersegurança, para fazer face à grande lacuna que o País tem. É também um diploma de formação avançada. O nível mínimo de qualificações de entrada é um mestrado em engenharia informática, de redes ou de sistemas e com-

putadores.

CW - Quando irá começar?

JT - Ainda não há data definida. Temos desenvolvido contactos com empresas para conseguirmos reunir as condições para a admissão e frequência de 40 alunos na primeira edição do curso, em dedicação exclusiva durante seis meses.

Isto só será possível se lhes forem dadas condições adequadas a tal situação, à partida, nomeadamente através de vínculos contratuais que assegurem um salário mensal e o pagamento dos custos da frequência do curso.

CW - O que está a impedir o arranque?

JT - Desenhámos um curso de seis meses, intensivo, que deverá ser pago pelo mercado. Estamos a falar com as empresas, porque, para pôr este curso a andar e para o afinar preciso de pelo menos umas oito edições durante quatro anos. A 30 pessoas por semestre, "fabricaríamos" 240 em quatro anos. Mesmo que metade sejam aspirados para o estrangeiro, sempre ficamos com 120 no País.

No entanto, alguém tem de lhes pagar para estudar e viver durante o curso. E as empresas não podem dispensar os poucos recursos que têm durante tanto tempo. Terão de ser pessoas novas. Para isso, as empresas têm de trabalhar em conjunto, com o nosso apoio, para recrutar pessoas, pagar-lhes, mete-los cá.

Se 15 empresas colocarem dois alunos por semestre é fácil. Mas é preciso que queiram. No entanto assinalo que é um imperativo nacional, que tem de suceder, o País precisa de matéria-prima.

CW - Já conseguiu conquistar empresas para financiar e colocar formandos no curso?

JT - Temos já algumas empresas que manifestaram a sua intenção em participar nesta iniciativa nos moldes acima descritos, mas o seu numero é ainda insuficiente para assegurar o seu funcionamento em termos economicamente viáveis.

CW - Está então a criar um modelo inovador de captação de alunos?

JT - Na Leadership Graduate Academy estamos a tentar criar um mercado de oferta e procura entre entidades que têm necessidades e entidades que têm meios para aplicar para que as fábricas funcionem. É um espaço de cooperação no interesse nacional e no interesse de cada uma destas empresas.

Por cada linha de fabrico pretendemos criar "um clube" de fornecedores/ consumidores, de parceiros. Com um contrato de fornecimento de, por exemplo, dois recursos por ano, durante quatro anos.

As empresas entregam a matéria-prima e nós devolvemo-los com competências adicionais. Os alunos poderão resolver problemas concretos das empresas em causa.

A falta de recursos humanos formados em cibersegurança; será talvez o maior impedimento à criação de riqueza no nosso país durante próximos anos, considera José Tribolet

CW - Qual poderá ser o caminho posteriormente?

JT - Se conseguirmos avançar, poderemos, facilmente, mobilizar os nossos colegas de Coimbra, Porto, etc, e escalar este exemplo. E depois fazer uma rede de franchising com os politécnicos e fazemos soldados em série. Porque aí precisamos de milhares.

CW - E o financiamento?

JT - Não pretendemos dinheiro. Queremos fazer avançar o curso, com a cooperação das empresas que podem arranjar o dinheiro onde quiserem. Não queremos intermediários. Se os parceiros quiserem ir buscar os milhões para a transformação digital destinados à formação ao Instituto de Emprego e Formação Profissional (IEFP) ou ao Ministério da Economia, anuncia-

Cinco maneiras de tornar mais seguro o comportamento dos funcionários

Algumas pessoas aprendem visualmente e outras mais pelo discurso. Para muitos, tem de haver uma combinação de ambos. Fazer exercícios práticos pode ajudar.

Enquanto alguns especialistas consideram ser nas empresas e na auto-formação que se aprende mais sobre cibergurança, Alan Usas, director do mestrado executivo em cibersegurança da Universidade de Brown, defende que a formação académica é fundamental.

Saber comunicar sobre cibersegurança é uma das valências cujas técnicas podem ser aprendidas nas universidades. Afinal, a cibersegurança é um domínio das TI, mas é também um problema organizacional.

Os responsáveis pela cibersegurança têm de conseguir comunicar o impacto e a dimensão que os ataques podem ter em termos comerciais, com perdas de receitas, de produtividade ou de rentabilidade para garantir que todos na empresa, incluindo a administração, compreendem os riscos e o impacto potencial das vulnerabilidades.

Das estratégias usadas sobressaem cinco formas de melhorar os cuidados dos funcionários com a cibersegurança:

1 - Para melhorar o comportamento dos empregados face à cibersegurança poderá provocar o erro e corrigir a pessoa. Pode selecionar um grupo de pessoas de cada departamento a quem enviar um e-mail de phishing personalizado, utilizando um endereço de email externo. Deverá utilizar apenas informações passíveis de serem obtidas em redes sociais. Pode enviar um convite para apoiar a equipa de que o colaborador é adepto. Ao clicar no link o colaborador será encaminhado para as melhores práticas de forma positiva.

2 - O departamento de marketing poderá ajudar na comunicação com os funcionários. Os conhecimentos de comunicação desses profissionais de comunicação, que sabem como comunicar com diferentes públicos, pode ser aplicado para fazer chegar mensagens de segurança aos públicos internos da organização. Crie um plano de comunicação em que ambas as equipes possam executar e monitorizar os métodos mais eficazes.

3 - Já parou para pensar que a forma como a mensagem está a ser comunicada poderá não estar a ser devidamente absorvida pelos utilizadores? Mude. Algumas pessoas aprendem visualmente e outras mais pelo discurso. Para muitos, é uma combinação de ambos. Vá alterando a forma como a mensagem de segurança é entregue aos funcionários. Comece com um e-mail mensal, uma sessão online ou por Intranet. Eleve o grau formação presencial. Ao utilizar esses diferentes meios ajudará a sua mensagem a repercutir em mais funcionários. A repetição, embora através de diferentes canais, contribuiu para que se retenha a mensagem.

4 - Torne a segurança relevante para os empregados. Quando uma grande empresa chegar às primeiras páginas dos jornais por uma violação de dados, resultado da abertura de um email infectado por um funcionário, comunique imediatamente como algo que poderia acontecer na sua empresa, com qualquer um dos funcionários. É oportuno, apelativo e estará no radar dos executivos.

5 - Recompense o bom comportamento. A segurança de TI está associada a desgraça e tristeza. Mas pode-se mudar essa percepção recompensando os funcionários pela detecção de uma ameaça ou falha de segurança. ■

Quatro sugestões para tirar partido do surto de Wanna Cry

Quando os incidentes de segurança chegam à imprensa generalista, pode aproveitar-se o momento para sensibilizar os recursos humanos.

Os surtos de Wanna Cry e de NotPetya são dois recentes eventos de falhas de segurança que ganharam visibilidade nos medias mais generalistas. Podem servir de alertas para os problemas da cibersegurança, mas a verdade é que já soaram outros alarmes do mesmo género, lamenta Ira Winkler consultor de segurança.

Claramente, estes dois recentes episódios só provaram que as lições não foram aprendidas. Mas são uma excelente oportunidade para consciencializar os recursos humanos.

Sempre que um grande ataque se tornar um dos principais tópicos das notícias, os responsáveis de programas de segurança devem ter em conta o que os funcionários estão a ouvir sobre o incidente e definir o que eles precisam de reter. Interessa sobretudo colocar as seguintes questões, diz Winkler.

A narrativa predominante está errada?

Quando se observa a informação disponível para o público, é necessário considerar se é rigorosa. O discurso geral pode dar às pessoas uma falsa sensação de segurança ou, pelo contrário, promover o medo, resultando em inacção. Tem de se perceber como é que os utilizadores entendem o ataque para perceber se é necessário mudar a percepção que têm do evento. Ou avançar para outra medida.

A informação veiculada está a fazer com que as pessoas se sintam inatingíveis?

Quer um problema ou ataque afecte ou não os utilizadores, é necessário compreender se eles acreditam que a questão tem algum impacto sobre eles. Se não o fizerem, vão ignorar o que pode ser um incidente importante ou, pelo menos, ignorar os esforços de sensibilização relacionados com o problema que se propõem.

O pretende que as pessoas conheçam sobre os ataques?

Quer o incidente envolva especificamente as TI da empresa quer esteja apenas relacionado com o utilizador, há sempre uma lição a transmitir. Por exemplo, mesmo que o malware "Heartbleed" actuasse no servidor e os utilizadores não pudessem fazer nada para corrigir a situação, foi uma óptima oportunidade para demonstrar a importância de mudar regularmente de password.

Na mesma linha, o Wanna Cry foi uma oportunidade para informar os utilizadores sobre a importância de aplicar "patchs" nos computadores domésticos e de trabalho. Há sempre lições a tirar, directa ou indirectamente.

Como é que o discurso afecta os utilizadores?

Antes de tomar qualquer acção, convém determinar como são os utilizadores afectados pelos eventos. Estão em risco? Existem medidas que precisam de tomar? Há alguma lição a extrair? O incidente afecta os utilizadores em casa ou no trabalho? Afecta as suas famílias?

Consciencializar, sensibilizar, motivar

Depois de perceber que pontos merecem enfoque, interessa determinar a melhor maneira de os promover. Segundo Ira Winkler, existem três etapas para alterar o comportamento do utilizador: consciencializá-lo para o problema, sensibilizá-lo para a solução e motivá-lo para implementar a solução. O último é o passo mais crítico.

Quando há um incidente com direito a "manchete" existe mais motivação do que habitualmente. Mas raramente as notícias se concentram nas soluções simples. Concentram-se no problema assustador. Contudo essa é uma motivação incrível sobre a qual importa construir soluções. ■