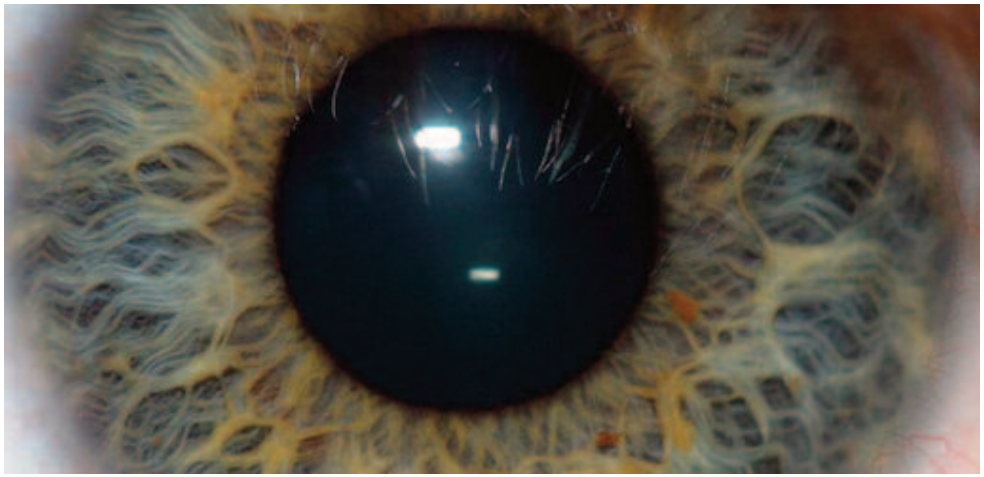
DOSSIER FEVEREIRO 2014

COMPUTERWORLD

SEGURANÇA



COMPUTERWORLD www.computerworld.com.pt
Av. da República, N.º 6, 7º Esq. 1050-191 Lisboa
Director Editorial: **Pedro Fonseca** pfonseca@computerworld.com.pt
Editor: **João Paulo Nóbrega** jnobrega@computerworld.com.pt
Director Comercial e de Publicidade: **Paulo Fernandes**
pfernandes@computerworld.com.pt Telef. / Fax +351 213 303 791
Todos os direitos são reservados.

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 negócio, de consumo, entretenimento digital e videojogos. Anualmente, a IDG produz mais de 700 eventos e conferências sobre as mais diversas áreas tecnológicas. Pode encontrar mais informações do grupo IDG em www.idg.com

3 MOBILIDADE RASGA VULNERABILIDADES
A adopção de dispositivos móveis no acesso aos sistemas de informação das empresas será o foco principal de desafios para os gestores de segurança, em 2014, de acordo com vários responsáveis do sector. As formas de lidar com o problema variam.

7 BIOMETRIA GANHA IMPULSO
O domínio da biometria deverá alargar-se aos dispositivos móveis, enquanto os sistemas de encriptação de informação tendem a atrair maior procura.

9 BIG DATA DE DOIS GUMES
Os sistemas de Big Data criam necessidades no âmbito da segurança. Mas também podem revelar muita informação útil para a gestão das protecções.

10 CIBERCRIMINOSOS ESPECIALIZAM-SE MAS DIVERSIFICAM OPERAÇÕES
Alguns grupos que operam actualmente na fraude bancária deverão continuar a avançar para esquemas mais rentáveis, como os de sequestro de sistemas (ransomware), segundo projecções da Kaspersky.

11 CSO PRECISAM DE PERCEBER MELHOR AS AMEAÇAS
A modelação de ameaças parece ser a prática mais adequada. As organizações precisam de quantificar os seus riscos o melhor que podem, de forma periódica, até para evitar decisões baseadas na emoção.

14 NEGAR A INSEGURANÇA JÁ NÃO É "SOCIALMENTE ACEITE"
A necessidade de proteger as infra-estruturas críticas é vista com maior importância em Portugal, assinala Lino Santos, director do CERT.PT. Mas os índices de ciberciminalidade não são baixos e há muito a corrigir no sistema judicial. É preciso ainda investir em tecnologia para os sistemas do Estado e na formação.

17 A EVOLUÇÃO DA SEGURANÇA FÍSICA
A segurança física já percorreu um longo caminho desde o advento da fechadura e da chave. Mas em todas as suas alterações, o maior aspecto da evolução da segurança física foi como se integrou no mundo digital.

MOBILIDADE RASGA VULNERABILIDADES

A ADOPÇÃO DE DISPOSITIVOS MÓVEIS no acesso aos sistemas de informação das empresas será o foco principal de desafios para os gestores de segurança, em 2014, de acordo com vários responsáveis do sector. As formas de lidar com o problema variam.

A encriptação, biometria em dispositivos, as soluções para políticas seguras de BYOD - nas quais se incluem as aplicações de gestão de dispositivos móveis -, são vistas como áreas de potencial dinâmica no segmento da segurança durante 2014, por vários responsáveis do sector das TIC em Portugal. Diversos factores estão a produzir mudanças relevantes no quadro dos sistemas da informação e emergem lacunas merecedoras de atenção.

Mas a necessidade de suportar o acesso seguro e a gestão da informação, em contexto de mobilidade, estará na base de grande parte das preocupações. Isso não quer dizer que não haja outros focos, associados à conformidade com regulamentos, por exemplo.

As soluções assumem várias formas conforme os quadrantes tecnológicos dos fornecedores. Rui Melo Biscaia, gestor de desenvolvimento de produto da Watchful, considera que "a indústria está num processo de mudança de segurança centrada na rede para segurança centrada nos dados".

Há vários anos que o sector fala desta transição. Mas actualmente esta parece ter um maior impulso.

Segundo este responsável, à mudança está associada a migração para "o paradigma da cloud computing e a utilização de dispositivos móveis", segundo estratégias de BYOD. Já Hugo Abreu, director-geral da Oracle, destaca também a utilização das redes sociais ou as aplicações de Big Data como elementos transformadores.

"O sequestro de contas de utilizador passará a ser mais frequente e não apenas em redes como o Twitter, mas também em sites orientados a negócios, como o LinkedIn", confirma Rui Duro, gestor de vendas da Check Point, em Portugal.

De outra perspectiva, há os riscos sobre a segurança interna de dados sensíveis. Embora tenha estado sempre presente os funcionários são reconhecidos como a maior ameaça à segurança dos dados , nos últimos tempos os fornecedores de tecnologia têm insistido neste tema, incrementando os seus alertas.

Empregados como instrumentos

A Check Point, por exemplo, "acha que se irão destacar a engenharia social, as campanhas de malware dirigidas, as botnets ou as ameaças internas, ou seja, os ataques às empresas a partir de dentro, usando os seus próprios empregados como instrumentos", antecipa Rui Duro. Na perspectiva deste responsável, a engenharia social através do email permanecerá como o método preferido para lançar ataques de malware ou de phishing.

"Os ataques e episódios a partir de dentro das empresas e dirigidas a instalações e infra-estruturas públicas, vão obrigar a redefinir a abordagem à segurança, segmentando mais as redes, aumentando a inspecção de código nocivo e ataques dentro da rede da mesma forma que até agora na periferia", sugere.

Neste quadro, e de acordo com a estratégia da Watchful, as "tecnologias que aplicam a segurança e protecção da informação diretamente nos dados - tais como classificação dinâmica dos ficheiros, IAM, e gestão de politicas associadas à aplicação de direitos sobre a informação" irão tornar-se mais relevantes, defende Rui Melo Biscaia, da Wachtful.

Dispositivos de conteúdo cada vez mais valiosos

Entre os responsáveis consultados, as aplicações e o tema da gestão dos dispositivos móveis obtêm o maior número de referências. "As soluções de Mobile Device Management (MDM) e mais recentemente as de Mobile Access Management (MAM) têm vindo a registar uma procura crescente, sendo expectável que se venha a acentuar ainda mais durante os próximos anos, tendo em consideração a explosão do tráfego de dados que se irá registar nas plataformas móveis", considera Hugo Abreu.

As aplicações MAM permitem disponibilizar um "container" - ou contentor ou área virtual delimitada e protegida -, no qual são alojadas as versões de mobilidade das aplicações corporativas. "O acesso a essas aplicações é controlado de forma centralizada pelas organizações, e de acordo com as políticas de segurança associadas a cada utilizador", explica o responsável da Oracle. É também uma maneira de estabelecer uma fronteira entre a utilização pessoal e o uso profissional.

"Os dispositivos móveis estão na mira dos cibercriminosos por serem ferramentas de trabalho cada vez mais populares e a sua utilização é cada vez maior", alerta Patrícia Esteves, directora de marketing da Panda. "São cada vez mais valiosos por armazenarem informações confidenciais e pessoais, como as passwords de acesso, códigos" ou outros. O investimento em MDM será um dos principais pólos de crescimento do segmento, em 2014, segundo esta responsável.

Ameaças na mobilidade aumentam

De uma perspectiva centrada num contexto mais externo, a segurança dos dispositivos móveis, de tablets e smartphones, ganha ainda maior relevância, segundo o consultor da Kaspserky Labs, Vicente Diaz. "O número de software nocivo destinado a smartphones deverá aumentar, e surgirão novos troianos bancários, para mobilidade, sem necessidade de basearem em infecções prévias de PC", prevê.

No entanto, o director de consultoria de segurança da Unisys, Sérgio Sá, considera que "a utilização de equipamentos pessoais para acesso à informação da organização, promete continuar a crescer". E o cenário agrava-se, teoricamente, com outra tendência: os proprietários dos equipamentos vão começar a implantar os controlos de segurança nos dispositivos.

"Provavelmente irão pôr em causa ou limitar as capacidades dos controlos de segurança da organização", alerta o consultor. Não admira por isso que o director de tecnologia da Microsoft, Miguel Caldas preveja que a segurança e a privacidade nas plataformas móveis (ou a falta delas) vão estar cada vez mais expostas. ■

DÊ LIBERDADE E SEGURANÇA AOS SEUS COLABORADORES PARA ESTAREM SEMPRE LIGADOS À ORGANIZAÇÃO

Bruno Berrones
Gestão de Produto Segurança PT

A mobilidade faz hoje parte da vida das pessoas, integrando a sua vida pessoal e profissional. A utilização crescente de smart devices, dentro e fora do local de trabalho, mudou totalmente a forma como as pessoas interagem e trabalham.

Neste contexto, gerir todo o potencial das tecnologias móveis passou a ser crucial para as organizações aumentarem a sua produtividade e eficiência.

Para implementarem esta mudança, as organizações necessitam de definir como ultrapassar alguns obstáculos, tais como a configuração e a gestão dos dispositivos, a segurança e a proteção da informação e a convivência de dados corporativos com dados pessoais no mesmo equipamento.

Existem muitas abordagens tecnológicas disponíveis com vista à integração dos dispositivos móveis no ambiente corporativo. Porém, a diversidade de opções dificulta a escolha por parte das organizações, preocupadas em proteger o seu investimento e definir soluções para o futuro.

Neste impasse, os colaboradores continuam a querer explorar todas as funcionalidades dos seus equipamentos e os departamentos de tecnologias de informação precisam de um sistema robusto, de simples e rápida instalação, que lhes permita garantir a segurança dos dispositivos e dos dados móveis.

Ao possibilitarem uma implementação com impacto mínimo nos sistemas de informação da organização, as soluções de MDM (Mobile Device Management) permitem proteger e gerir, de forma integrada, todos os terminais móveis e controlar o acesso remoto à rede corporativa através da implementação transversal de políticas de segurança, tais como encriptação de dados, validação de aplicações, controlo de acesso a conteúdos, entre outras.

A gestão dos equipamentos passa a ser efetuada centralmente pelo administrador de sistemas que administra todos os equipamentos móveis utilizados pelos colaboradores, separando os conteúdos pessoais dos empresariais.

Ao utilizarem as soluções de MDM na cloud, em modelo de Software as a Service (SaaS), as organizações conseguem reduzir custos e usufruir de um serviço capaz de evoluir à medida das suas necessidades.

Sem implicar qualquer investimento inicial, estas soluções são implementadas online em apenas alguns minutos e não requerem a instalação de hardware. O serviço é totalmente escalável, possibilitando aumentar ou diminuir a capacidade de forma flexível, com um custo de utilização por terminal.

Na cloud, a gestão centralizada de todos os terminais, aplicações e serviços móveis pode ser realizada, em qualquer lugar, a partir de uma consola de fácil utilização, acessível através de um browser com acesso à internet. A plataforma MDM e a informação passam a estar protegidas num data center que garante todos os aspetos críticos de segurança. Simultaneamente, a plataforma é operada de forma totalmente integrada com os sistemas corporativos internos, tais como Active Directory e Entreprise Data, permitindo a sua total assimilação pela organização.

Os gestores das organizações deixam assim de se preocupar com a gestão da tecnologia e da segurança, podendo focar-se em proporcionar mais mobilidade às suas equipas com mais e melhores ferramentas de trabalho.

Porquê a PT?

A PT ajuda as organizações a desenvolverem a sua estratégia de mobilidade de forma flexível e sem preocupações com tecnologia, adequando os recursos às características e à evolução da sua atividade. Para isso, disponibiliza aplicações móveis corporativas, soluções de gestão de mobilidade empresarial, serviços de gestão TI e capacidade de banda larga com suporte na sua rede de fibra e 4G/LTE, com total cobertura nacional. As Soluções Cloud da PT estão suportadas na maior rede de data centers do país, potenciando redução de custos com as TI, aumento de produtividade e mobilidade, com elevados níveis de sustentabilidade.

PT Empresas

ptempresas.pt

BIOMETRIA GANHA IMPULSO

O DOMÍNIO DA BIOMETRIA deverá alargar-se aos dispositivos móveis, enquanto os sistemas de encriptação de informação tendem a atrair maior procura.

"A introdução da autenticação por impressão digital nos iPhone promete revolucionar a indústria da biometria e levar à sua massificação, de forma a proteger os dispositivos e dados, deixando para trás o tradicional [modelo de] utilizador/password", considera Sérgio Sá, da Unisys. Mas o impulso dado à área da biometria não deverá restringir-se a esse tipo de autenticação baseada no corpo dos utuilizadores. De acordo com este responsável, as tecnologias de identificação pela íris e o reconhecimento facial já estão suficientemente maduras.

No entanto, o desafio é tornar as novas abordagens de autenticação com múltiplos factores (com a substituição desse modelo de utilizador/password) "o menos impactante" possível, considera Rui Melo Biscaia, da Watchful.

A viabilidade económica também é uma questão importante, capaz de ser resolvida com a biometria comportamental.

Sérgio Sá considera que a biometria nos dispositivos móveis deverá abrir caminho para a sua utilização noutros serviços online. Os contextos de e-commerce e de banca online afiguram-se com potencial para isso. Rui Melo Biscaia lembra que o Facebook e a Google também já investiram em sistemas de

> **A viabilidade económica também é uma questão importante**

autenticação com múltiplos factores.

Caso Snowden favorece encriptação

"Depois do problema de confiança levantado por Snowden, veremos um re-investimento em encriptação", prevê Miguel Caldas, da Microsoft. Também Sérgio Sá considera que, "possivelmente", essa área estará entre as de "forte crescimento".

O consultor norte-americano Edward Snowden revelou em 2013 práticas de vigilância da National Security Agency (NSA), que podem ter resultado em espionagem industrial.

"O reforço deverá acontecer, principalmente, com a informação e comunicações internas em que os controlos eram menos apertados ou inexistentes. No exterior, embora já existisse, provavelmente também será revisto, resultado da diversidade dos meios de comunicação e acesso à informação (dispositivos móveis)", concretiza o responsável da Unisys.

Na mesma linha, Miguel Caldas prevê "um aumento generalizado de utilização da encriptação de nível elevado nas comunicações, tentando evitar a intrusão de serviços de informação apostados na recolha maciça de informação".

O director de tecnologia da Microsoft assinala que novas formas de encriptação (nomeadamente a homomórfica) deverão concentrar, em 2014, esforços de investigação. Os maiores intervenientes no mercado deverão avançar já com projectos-piloto, prevê este responsável. ■

> **Aumento generalizado de utilização da encriptação de nível elevado**

O IMPACTO DO FIM DO XP

Ao referir o fim de vida do Windows XP como evento com potencial de marcar a segurança das informações, Miguel Caldas (Microsoft) sugere a possibilidade de o fim do suporte "ter impactos significativos em muitas organizações". Mas, mais importante, Vicente Diaz (Kaspersky) recorda que as empresas (e utilizadores) deverão esperar um surto de infecções relevante, após 8 de Abril de 2014, data do fim generalizado de suporte ao XP pela Microsoft.

Não obstante, o fabricante do sistema operativo já prometeu que a mesma se manterá até 14 de Julho de 2015 para os clientes empresariais utilizadores de várias aplicações de segurança, que vão continuar a receber as actualizações para XP. ■

BIG DATA DE DOIS GUMES

OS SISTEMAS DE BIG DATA criam necessidades no âmbito da segurança. Mas também podem revelar muita informação útil para a gestão das protecções.

Um dos efeitos das soluções de Big Data é alargarem o conjunto de fontes de dados dos sistemas de datawarehouse a fontes externas, como as redes sociais.

"A utilização de fontes externas, e bem assim de informação não estruturada, vai obrigar à implantação de mecanismos transversais de auditoria a todos estes tipos de dados, e que sejam capazes de recolher dados não estruturados e estruturados, consolidando-os e armazenando-os para auditorias a realizar posteriormente", considera Hugo Abreu.

Paralelamente, lembra o responsável da Oracle, está a aumentar a exigência e a pressão por parte das autoridades nacionais e organismos internacionais (nomeadamente da Comissão Europeia) sobre garantias de privacidade dos dados pessoais que estão na posse de diferentes organizações, sejam elas públicas ou privadas.

O analista da Kaspersky, Vicente Diaz, confirma que deverão surgir novas normas de privacidade e isso vai atingir o sector público, mas também as empresas de infra-estrutura de TI que terão de tornar mais robustas as suas política de segurança, serviços e modelos de regulação de negócios.

Rui Duro recorda um efeito mais positivo das ferramentas de Big Data, assinalando as "tremendas oportunidades" que as soluções deverão proporcionar na análise de ameaças, envolvendo a correlação de eventos, o reporte de informação e a própria conformidade com os regulamentos.

Para este responsável da Check Point, a partilha de informação sobre as ameaças de forma colaborativa será um elemento-chave para garantir uma maior segurança e protecções mais actualizadas. "As plataformas unificadas de segurança e a consolidação da cloud computing" serão outros factores positivos, diz. ■

CLOUD "PROEMINENTE" NO DISASTER RECOVERY

As plataformas de cloud computing deverão conquistar "um lugar proeminente" nas estratégias para lidar com a prevenção de perdas de dados (Data Loss Prevention) e de Disaster Recovery, nas previsões de Miguel Caldas, da Microsoft.
Já Hugo Abreu (Oracle), considera que "as soluções dos Portais de Serviço na Nuvem, com capacidade para self-service (nomeadamente auto-registo, autenticação/SSO e autorização) irão ser o facilitador da democratização deste modelo de computação".
Apesar disso, Rui Melo Biscaia, da Unisys, considera que a adopção do modelo "continuará a levar o seu tempo". As preocupações relacionadas com a segurança e privacidade dos dados são as principais razões para isso. E as organizações deverão manter uma abordagem "híbrida".

CIBERCRIMINOSOS ESPECIALIZAM-SE MAS DIVERSIFICAM OPERAÇÕES

ALGUNS GRUPOS que operam actualmente na fraude bancária deverão continuar a avançar para esquemas mais rentáveis, como os de sequestro de sistemas (ransomware), segundo projecções da Kaspersky.

Haverá alguma especialização mas outras organizações, de acordo com o analista da empresa, Vicente Diaz, vão continuar a diversificar negócios. Tendem a procurar "melhorar capacidades para tirar proveito de outro tipo de negócio fraudulento", diz.

Outras previsões:

- embora haja alguns indicadores sobre a utilização de vários dispositivos, enquadrados na Internet das Coisas para fins fraudulentos, a Kasperksy acredita que ainda estão longe de obter um impacto muito grande. Mas considera provável a ocorrência de campanhas específicas capazes de tirar partido daqueles equipamentos;
- os hacktivistas tomarão contacto com outros grupos (principalmente cibercriminosos já estabelecidos) para aproveitar tácticas e recursos;
- os códigos nocivos direccionados aos utilizadores de smartphones devem aumentar;
- o número de aplicações de phishing bancário deve crescer;
- a fraude contra alvos de média e pequena dimensão tende a aumentar, incluindo os pagamentos eletrónicos, lojas online, sites de leilões e sociedades financeiras;
- o malware destinado a explorar sistemas POS específicos deverá melhorar. ■

AUSTERIDADE COMPROMETE INVESTIMENTOS EM SEGURANÇA

"Em 2013, um dos principais focos de investimento foi na visibilidade sobre eventos de segurança, para criar a capacidade de identificar e corrigir desvios às regras de segurança da organização e também para assegurar a conformidade regulamentar em alguns sectores de atividade", revela Pedro Galvão, gestor sénior de consultoria na IBM.
Na origem destes investimentos estiveram preocupações com a seguranças da informação, associadas à adopção das tecnologias de mobilidade. E a eficiência operacional na gestão da segurança está a ganhar destaque.
As soluções de segurança em mobilidade e de "security intelligence" estão a atrair muita atenção por parte de todas as organizações, confirma Pedro Galvão. Mas o tema da gestão "tem mais a ver com a forma de organizar a equipa e a forma de explorar a tecnologia existente". As soluções geridas parecem ser uma opção a considerar e permitem um maior enfoque "em áreas de segurança aplicacional por recursos internos".
Não obstante a visão da IBM, segundo a qual muitas empresas continuaram em 2013 a investir em segurança, Patrícia Esteves, da Panda, afirma que "com as diferentes medidas de austeridade nos últimos anos, muitas entidades portuguesas não conseguem acompanhar" a evolução, ficando com "o parque informático cada vez mais obsoleto".

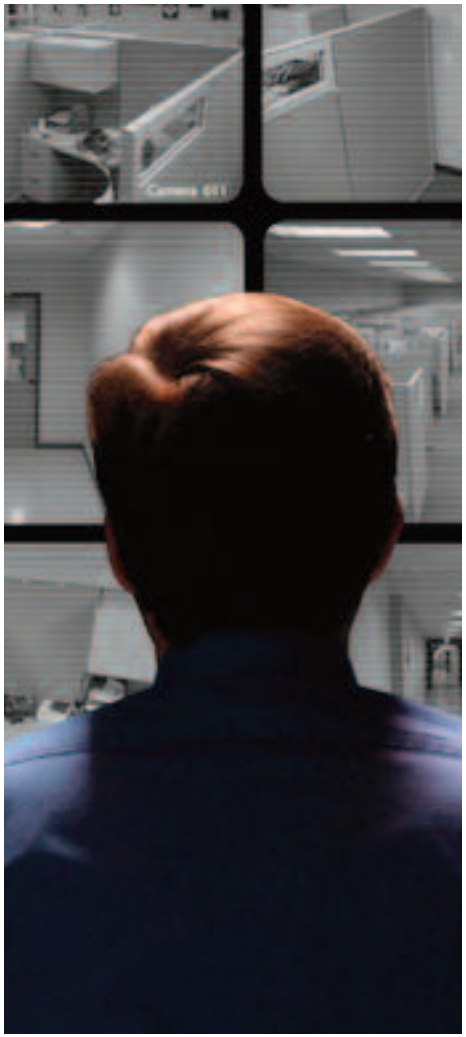
CSO PRECISAM DE PERCEBER MELHOR AS AMEAÇAS

A MODELAÇÃO DE AMEAÇAS parece ser a prática mais adequada. As organizações precisam de quantificar os seus riscos o melhor que podem, de forma periódica, até para evitar decisões baseadas na emoção.

Com a ocorrências de violações significativas de segurança a tornarem-se quase diárias, torna-se claro que os atacantes estão a conseguir ficar um passo à frente de muitas organizações. E é evidente que os profissionais de segurança (CSO) e os CIO não se estão a concentrar o suficiente sobre as ameaças e os dados mais importantes.

Considerem-se os resultados do mais recente estudo mundial e anual da PricewaterhouseCoopers e da revista CSO sobre a segurança de informação. De acordo com os mais de 9.600 executivos entrevistados, as suas organizações têm aumentado os gastos com segurança de TI, mas o número de ataques a que estão a resistir e os custos inerentes aos mesmos são crescentes.

Portanto, não é tão surpreendente saber que apenas 17% dos entrevistados se preocupam em classificar o seu uso comercial de dados, cerca de 20% têm procedimentos dedicados à protecção da propriedade



intelectual e 26% (número surpreendentemente baixo) para activos de estoque ou para gestão de activos. Se as empresas quiserem melhorar, precisam de perceber com maior precisão as ameaças reais prontas a incidir sobre as suas organizações e as vulnerabilidades de TI na sua empresa. Qual é a forma de corrigir a situação? A modelação de ameaças.

A realização de avaliações de risco e de modelos de ameaças não é um conceito novo. "Todos fazemos avaliações de conduta de risco e modelos de ameaças nas nossas vidas diariamente, se pensarmos bem. Imaginamos quem poderia querer roubar o nosso carro ou assaltar a nossa casa", diz Wendy Nather, directora de pesquisa em segurança empresarial, da 451 Research.

Nem sempre somos bons nisso - por exemplo quando temos mais medo de ataques de tubarão do que de acidentes

perto de casa. As pessoas tendem a ficar mais nervosas quando embarcam num avião, do que quando se sentam atrás do volante do seu carro.

Gestão emocional de riscos

As emoções assumem o controlo, muitas vezes também nas empresas. Para melhorar as suas decisões, as organizações precisam de quantificar os seus riscos o melhor possível.

A tomada de decisão baseada na emoção deve ser evitada. "Do ponto de vista organizacional, é importante porque uma empresa precisa de perceber quais são e o que são essas ameaças, assim como uma pessoa deve querer saber quem são os seus concorrentes, capazes de constituir uma ameaça competitiva", diz Eric Cowperthwaite, vice-presidente para a segurança avançada e estratégia da Core Security e ex-CISO da Providence Health and Services, em Renton (EUA).

> **Os bancos têm feito a modelação de ameaças de fraude desde sempre**

"Caso contrário, o CEO fica sempre inundado por toda a fantasia das notícias quotidianas", considera. A modelação de ameaças não é um conceito novo para alguns mercados verticais, tais como o dos serviços financeiros e das infra-estruturas críticas ou do fornecimento de serviços críticos. "Os bancos têm feito a modelação de ameaças de fraude desde sempre", diz Nather.

"Porém, acho que, com o passar do tempo, a indústria aprendeu que tem um modelo de ameaça maior do que apenas a fraude", diz. Faz sentido, as condições de negócio, as ameaças e as vulnerabilidades estão sempre a mudar.

ELEMENTOS NECESSÁRIOS VARIAM

Quais são os elementos necessários para um modelo de ameaça? Varia conforme envolva líderes empresariais, as equipas de desenvolvimento, as de operações ou as equipas de segurança, na classificação da importância dos dados, das aplicações e das infra-estruturas para o negócio.

A equipa de segurança também pode identificar vulnerabilidades dentro das aplicações e dos sistema, e os potenciais cibercriminosos que gostariam de atacar. Ao listar estes intervenientes associados às ameaças, é importante não ficar a pensar que cada ameaça é um risco potencialmente significativo para a organização.

"Não se trata de ter defesas contra todas as ameaças possíveis", diz Wendy Nather, da 451 Research, "mas apenas para aquelas mais prováveis". Como é que os cibercriminosos poderão procurar atingir a sua organização? Bandos à procura de informações financeiras , hacktivistas interessados em desfigurar o site da empresa, ou Estados à procura de segredos comerciais, como poderão provavelmente tentar alcançar os seus objectivos? Com base numa avaliação de vulnerabilidades e de riscos, qual é a probabilidade de terem sucesso? Feche as maiores, mais importantes lacunas associadas às maiores ameaças e vulnerabilidades primeiro.

Frequência gera maior precisão

É por tudo isto que os modelos de ameaças periódicas são necessárias. Por exemplo, quando se trata de bancos e serviços financeiros, Nather explica que, quanto mais as suas transações de clientes passaram para o online, os bancos tiveram de ter em conta os elementos de autenticação dos seus clientes e como eles podem ficar comprometidos, ou mesmo como os seus clientes podem também tentar cometer fraudes.

Quando Cowperthwaite foi CISO, fazia regularmente um modelo de ameaças para obter uma melhor compreensão dos riscos subjacentes à organização, e para acalmar as reacções emocionais mais comuns a notícias de quebras de segurança. Queria também poder dar melhor enfoque aos seus gastos com segurança.

"O valor da modelação de ameaças tanto para o CISO como para a organização é principalmente a capacidade de gerir de forma mais eficaz e eficiente os riscos", considera. "A maioria dos programas de segurança de hoje, pelo menos, procura basear-se no risco, e simplesmente, um risco é uma ameaça externa, interna ou ambiental, associada a uma vulnerabilidade".

"A modelação de ameaças é importante para determinar aquelas capazes de atingir a organização, e saber o nível de preparação da mesma face a essas ameaças específicas. Caso contrário, acaba-se por se estar a tentar proteger a organização contra tudo", diz.

Cowperthwaite lembra a altura quando a notícia em torno de cibercriminosos patrocinados por Estados surgiram pela primeira vez, tendo como alvo principalmente as empresas de tecnologia na época. "Porque reagiram emocionalmente, toda a gente saíu a correr pensando que o céu estava a cair", explica. "Não estavam a avaliar bem a possibilidade daqueles ataques específicos terem como alvo a sua organização. Nem procuraram olhar para um modelo de ameaças adequado sobre quem os atacantes estavam realmente a atacar, o que queriam, e quais eram as suas capacidades".

"No meu modelo de ameaça, não considerei esses atacantes como um risco devido ao modelo da sua ameaça e comportamento. Eu estava numa organização sem fins lucrativos, e não parecíamos ter qualquer coisa de valor para eles e por isso concluímos que não eram um risco significativo para nós", explica Cowperthwaite. ■

A modelação de ameaças é importante para determinar aquelas capazes de atingir a organização, e saber o nível de preparação da mesma face a essas ameaças específicas. Caso contrário, acaba-se por se estar a tentar proteger a organização contra tudo

NEGAR A INSEGURANÇA JÁ NÃO É "SOCIALMENTE ACEITE"

A NECESSIDADE DE PROTEGER as infra-estruturas críticas é vista com maior importância em Portugal, assinala Lino Santos, director do CERT.PT. Mas os índices de ciberciminalidade não são baixos e há muito a corrigir no sistema judicial. É preciso ainda investir em tecnologia para os sistemas do Estado e na formação.

Portugal está num patamar diferente quanto à atitude assumida no tema da segurança dos sistemas de informação, considera o director do CERT.PT, Lino Santos, mas falta ainda corrigir muitos aspectos, tanto na tecnologia como nas pessoas e no sistema judicial, que têm de ser melhor capacitados.

Apesar de o espaço português ser uma zona-alvo secundária, os índices de ciberciminalidade não são baixos. Sem arriscar previsões, confirma o potencial de vulnerabilidades associado aos dispositivos móveis, e sublinha a crescente ameaça resultante do aproveitamento de recursos por parte dos criminosos: há uma melhor

LINO SANTOS
DIRECTOR DO CERT.PT

conjugação de velhas técnicas com a capacidade de processamento e de transmissão.

Computerworld - Alguns analistas dizem que 2014 pode ser um ano particularmente activo na ciberciminalidade. Concorda? Faz sentido para o espaço português?

Lino Santos - Não consigo responder directamente à pergunta. Era preciso uma bola de cristal. Se analisarmos o ponto de vista da motivação, Portugal continuará a ser um alvo secundário.

Temos menos dinheiro e, considerando os custos de localização como a língua, somos pequenos, quando comparados com outros potenciais alvos. Deve no entanto ser excluída desta conclusão os muitos grupos dedicados ao cibercrime de brasileiros.

Do ponto de vista da capacidade e apesar dos espetaculares incidentes noticiados nos últimos anos, tecnicamente pouco ou nada de novo surgiu no quadro dos vectores de ataque. A última grande novidade foi, talvez, o aparecimento de malware polimórfico. Já lá vão alguns anos.

O que temos visto é uma cada vez uma melhor

conjugação de velhas técnicas aliada ao aumento de capacidade de processamento e de transmissão. Portanto, a não ser que surja um novo vector de ataque que altere radicalmente o quadro de ameaça, não consigo prever grandes alterações para 2014.

Não quero com isto dizer que os níveis de ciber-criminalidade são baixos. Longe disso. Ainda há um longo caminho a percorrer na consciencialização e na formação das pessoas, no investimento em tecnologia e processos de segurança da informação nas empresas e no Estado, bem como na capacitação do nosso sistema judicial na prossecução deste tipo de crimes.

CW - Vários fabricantes têm alertado para a emergência de malware dirigido a plataformas de mobilidade e diz-se que em 2014 os ataques a dispositivos móveis terá um grande incremento. Outros alertam para os riscos inerentes à Internet das Coisas e para as ameaças a infra-estruturas críticas. Que relevância têm, para o tecido empresarial português, estas duas supostas tendências?

LS - É um facto que ao longo dos últimos anos as empresas de soluções de segurança têm vindo a projectar este tipo de tendências: o crescimento da ciberconflitualidade nos dispositivos móveis, infra-estruturas críticas, cloud computing e, mais recentemente, na Internet das coisas.

Colocando de parte que estas mesmas empresas são as principais beneficiárias deste discurso, é natural que os ataques visando dispositivos móveis – pegando aqui neste exemplo em particular – apresentem um maior crescimento. Por um lado, a tecnologia de smartphones é mais recente do que por exemplo são os computadores pessoais ou os computadores portáteis.

Por outro lado, os mecanismos e processos de segurança desenvolvidos para estes dispositivos não apresentam o grau de maturidade já atingido por outro tipo de tecnologias. Acresce em cima destes factores o chamado "time-to-market" – um dos maiores inimigos da segurança –, muito mais curto nos smartphones do que noutro tipo de dispositivos.

Em suma, os dispositivos móveis são mais vulneráveis e naturalmente o número de ataques crescerá na medida da sua utilização e do valor da informação neles armazenada ou transmitida.

Outro "departamento" é o da segurança das infra-estruturas críticas. No plano internacional temos vindo a assistir à entrada de actores

Objectivos do CERT.PT

Os objectivos do CERT.PT são, a par da gestão adequada da rede CSIRT:

- estabelecer a confiança entre responsáveis pela segurança informática para criar um ambiente de cooperação e assistência mútua no tratamento de incidentes;
- criar indicadores e informação estatística nacional sobre incidentes de segurança para identificar contra-medidas;
- implantar instrumentos de prevenção e resposta rápida num cenário de incidente de grande dimensão;
- promover uma cultura de segurança em Portugal.

> **Em Portugal, "sentimos um incremento no número de ataques do tipo negação de serviço e um maior número de casos de ransomware"**

estatais e ao aumento das capacidades de actores não estatais. Convém, no entanto, realçar o caminho percorrido nesta matéria em Portugal. Nos últimos anos foi feito, por várias entidades oficiais e outras organizações, um grande esforço de alerta e consciencialização relativa a este assunto junto dos responsáveis pela administração e operação de infra-estruturas críticas nacionais.

O facto é que, hoje em dia, já não é "socialmente aceite" o discurso de negação do problema como acontecia há muito poucos anos; muitos operadores criaram capacidades de resposta a incidentes, bem como planos de continuidade de negócio; trabalham em redes formais ou informais, nacionais ou internacionais, para melhorar as suas capacidades. Ou seja, estamos num patamar de maturidade muito diferente daquele onde estávamos há poucos anos atrás.

CW - Quais foram as principais tendências de 2013, em Portugal, em termos de cibercriminalidade e segurança da informação nas empresas?

LS - Contamos terminar o relatório de 2013 em breve, mas empiricamente diria que dos eventos e incidentes de segurança tratados pelo CERT.PT, sentimos um incremento no número de ataques do tipo negação de serviço (como vítimas e como origem dos ataques) e um maior número de casos de ransomware (nestes como vítimas).

CW - Como evoluiu o grau de sofisticação das ameaças detectadas em Portugal? Tende a haver um aumento muito grande em 2014?

LS - Não temos esses dados. Não trabalhamos as ameaças, trabalhamos os incidentes. ■

A rede SIRT

A Rede Nacional de Computer Security Incident Response Services (CSIRT) - ou equipas de serviços de resposta a incidentes de segurança informática – inclui em Portugal as seguintes entidades:

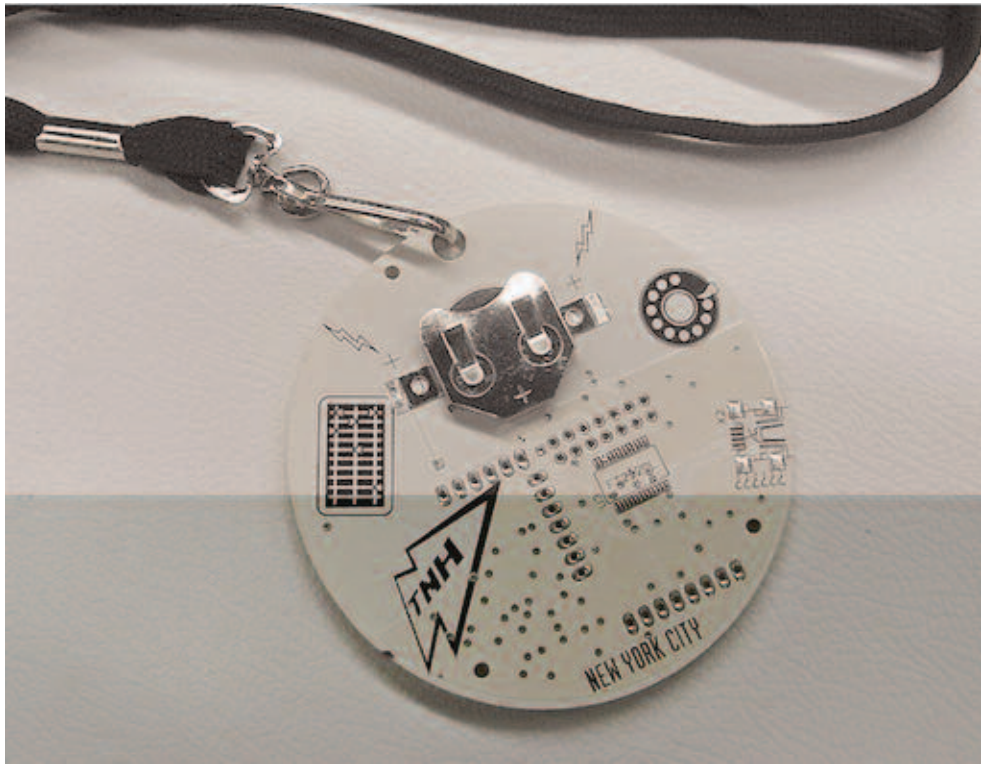
- Cabovisão /Oni Communications
- CC-CRISI (EMGFA);
- CEM (Angra do Heroísmo);
- CERT.PT;
- CGD;
- Claranet;
- Dognaedis;
- EDP;
- FEUP;
- IGFEJ;
- Millenium BCP;
- NFSI;
- PT;
- PT Servidor;
- Refer;
- Sonaecom;
- UTIS;
- Vodafone.

A EVOLUÇÃO DA SEGURANÇA FÍSICA

A SEGURANÇA FÍSICA já percorreu um longo caminho desde o advento da fechadura e da chave. Mas em todas as suas alterações, o maior aspecto da evolução da segurança física foi como se integrou no mundo digital.

"O que estamos a ver é a fusão de espaços electrónicos e físicos", diz Chris Nickerson, fundador e consultor-chefe da Lares Consulting. "Já estamos longe da simples segurança física para trabalhar com os lados sociais e electrónicos e certificar de que uma pessoa é quem diz ser".

Mas com a evolução surge um novo conjunto de riscos e vulnerabilidades, dos quais apenas alguns conseguimos aprender a melhorar. Para que a segurança física funcione, precisamos de compreender as novas tecnologias que nelas estamos a incorporar. "Fizemos grandes avanços, mas temos vindo a adoptá-las sem as aprender, de modo que nos expusemos de uma forma que não tínhamos antes na segurança física", diz Nickerson à CSO. "O risco é entender o que se está a fazer, não como. Se sabe o que está a usar e o usa bem, então não há nenhum risco".



O que se segue são oito dos desenvolvimentos mais significativos que ocorreram ao longo do tempo no campo da segurança física, e como alguns deles ainda estão a ser aprefeiçoados.

1. Cartões RFID

A maioria dos edifícios incorpora actualmente de alguma forma cartões RFID. Os cartões, que contêm duas peças cruciais de informação - o código do site e o crachá de identificação pessoal - permite aos funcionários passar o seu cartão próximo de um scanner, para ter acesso a certas áreas. "São bons para saber quem está a entrar e durante quanto tempo", diz Nickerson. "O RFID tem algumas vulnerabilidades mas ainda é melhor do que as chaves reais,

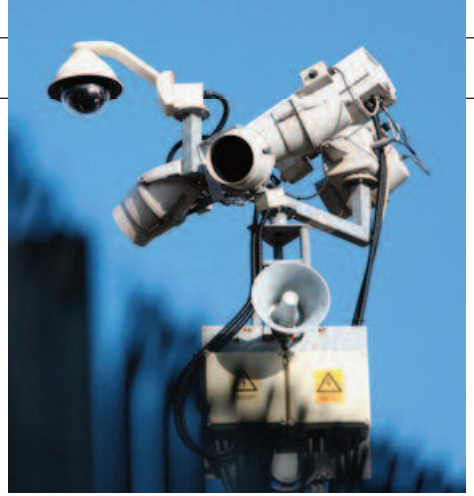
onde se consegue obter uma cópia de uma chave-mestra".

Na realidade, os cartões RFID estão cheios de falhas de segurança. Eles são facilmente clonáveis, por exemplo, e ataques de força bruta podem ser usados para aproveitar o facto de que os números de identificação do cartão são tipicamente incrementais (embora o outro aspecto, o código local, seja mais secreto). "A maioria das aplicações Web é 'inteligente' o suficiente para bloquear [o acesso, após várias tentativa fracassadas]", diz Nickerson. "Mas o RFID? Pode usar força bruta durante todo o dia. A maioria dos sistemas nem sequer o avisa se alguém tentou um milhão de vezes".

Além disso, algumas empresas colocam os seus sistemas RFID em fornecedores externos de cloud. Tudo o que um atacante tem de fazer é aceder a esse fornecedor e, de repente, tem acesso a todos os edifícios que usam o serviço em nuvem. "Estes são os sistemas de acesso electrónico padronizados que, ao terem algum tipo de servidores centralizados, podem 'falar' com todos os leitores" [dos cartões], refere Nickerson. "Num par de horas, conseguem-se encontrar todas as formas de abrir as portas".

2. Videovigilância

A videovigilância já existe há algum tempo mas melhorou drasticamente desde a sua criação. A videovigilância é agora sofisticada o suficiente para incorporar reconhecimento facial e videocâmaras com maior qualidade estão a criar imagens com maior resolução. "A alta definição [HD] é agora a norma e acima da HD está a tornar-se normal", diz Jay Hauhn, CTO e vice-presidente das relações com a indústria da Tyco Integrated Security. "As câmaras de megapixéis na video-segurança têm uma



muito boa imagem".

Mas com isto vem o grande desafio de fazer "streaming" em alta qualidade dessas imagens nas redes. "A largura de banda não é amiga quando se está a lidar com vídeo", diz Hauhn. "Pelo que também estamos a aproveitar os avanços da tecnologia no mundo do consumidores e a usá-la para conseguir distribuir mais vídeo".

3. Sistemas de segurança de perímetro

Já não é preciso depender exclusivamente de muros ou cercas para guardar o perímetro de uma instalação, graças aos avanços em sistemas de monitorização de perímetros. Alguns sistemas já utilizam microondas ou ondas de rádio para estabelecer um perímetro e podem alertar as equipas de segurança quando a área protegida está a ser invadida. "Pode-se ver quem está do lado de fora da área e ser alertado de antemão", diz Nickerson. "É um enorme avanço para o alerta precoce".

4. Reconhecimento da íris

Num equilíbrio entre ser preciso e não-invasivo, o reconhecimento de íris permite que as equipas de segurança possam identificar as pessoas com base apenas no padrão do seu olho. "Sou um grande fã do reconhecimento da íris, dado que os padrões são mais únicos do que o DNA", diz Hauhn. "As írises são realmente boas para serem registadas por uma câmara de alta resolução à distância".

Como o reconhecimento facial, é possível contornar a

tecnologia de reconhecimento da íris com uma fotografia do olho de outra pessoa, mas Hauhn sustenta que não se é tão facilmente enganado. Afinal, como realça Hauhn, "tente obter uma boa imagem de um olho e fazer isso".

5. Agentes de segurança e cartões de identificação com fotografia

Há algo a ser dito sobre as boas e antigas técnicas de vigilância com os dois olhos do ser humano. Com o uso de cartões RFID e os sistemas de acesso colocados em entidades externas, o elemento humano da segurança está a ficar esquecido. Saber quem acede ao edifício durante anos - ou, talvez, perceber que uma pessoa está a usar um cartão de identificação com uma foto de outra pessoa simplesmente porque o seu rosto não é o do cartão - são coisas que uma máquina não pode fazer, mas um ser humano sim.

"Esta relação com o ambiente é o que se está a perder", diz Nickerson. "Imagine que trabalhei durante 10 anos na recepção de um hotel. Conheço o seu rosto. Posso até ser capaz de dizer que você não deveria estar lá com base num 'feeling'. Muito disso está a ficar perdido".

6. Segurança ligada a dispositivos móveis

Não é raro nos dias de hoje ter sistemas de segurança - especialmente sistemas de segurança domésticos - ligados a um dispositivo móvel. Sensores inteligentes, trancas de segurança sem fios e sistemas remotos de controlo/manutenção podem ser controlados pelo dispositivo móvel do utilizador. Mas alguns dizem que, com uma tal conveniência, vem a segurança comprometida.

"Embora todos sejam formas convenientes e agradáveis para manter a sua casa 'segura', ao mesmo tempo é tudo através de um telemóvel, um dos principais alvos actuais dos ladrões, hackers, criadores de malware, etc.", diz Ryan Jones, consultor na Lares Consulting.

Embora os atacantes possam capturar fisicamente o telemóvel para obter as "chaves do castelo", "as pessoas parecem não se conseguirem ajudar ao perderem os seus telefones ou a tê-los roubados", diz Jones. "Antecipo um problema com assustar uma pessoa com o roubo do seu telemóvel e desbloquear a sua casa e desligar o alarme", acrescenta.

No curto prazo, Jones sugere que as pessoas tomem medidas de segurança simples para protegerem os seus sistemas de segurança, como o uso de bloqueio no telefone, no caso dele ser perdido ou roubado. Mas, a longo prazo, será preciso um melhor controlo de qualidade. "Tem-se esses executivos e celebridades que não bloqueiam os seus telefones, porque é inconveniente, mas as pessoas precisam realmente de usar [os bloqueios no telemóvel]", diz. "A longo prazo... quanto mais pessoas os comprarem, haverá provavelmente testes mais adequados feitos antes de serem colocados no mercado".

7. "Scanning" de impressões digitais

A digitalização de impressões digitais não só eleva o nível de segurança no ponto de acesso, exigindo identificação que é única para cada pessoa, como também permite que os sistemas de segurança possam manter o controlo de quem está a entrar num edifício. "Ele apenas é capaz de dizer que [essa pessoa] foi por esta porta nesse momento - há uma enorme

diferença entre isso que e 'é uma chave mas realmente não tenho ideia de quem era o seu proprietário'", diz Nickerson. "É o maior avanço que temos".

A tecnologia de "scanning" de impressões digitais está longe de ser perfeita, no entanto, porque as impressões digitais podem ser transferidas e copiadas usando materiais gelatinosos, por exemplo. Mas, como aponta Nickerson, os fabricantes de sistemas de segurança biométricos têm, por qualquer razão, feito grandes avanços na melhoria das suas falhas. "Os fabricantes começaram a colocar sensores de calor... e de pressão e mapeamento de calor no scanner", diz. "E agora o exame também tem que combinar a estrutura venosa da pessoa. São estes múltiplos factores de autenticação que fizeram tão grande a biometria".

8. Reconhecimento facial

Parte dos avanços que têm sido feitos na videovigilância é a codificação do reconhecimento facial. O reconhecimento facial tornou-se tão avançado que não só pode ser usado para verificar se alguém é quem diz ser como também pode ser usado para escolher uma pessoa para a retirar para fora de uma multidão.

Apesar das falhas, a tecnologia está avançada o suficiente para ser fiável

"Pode-se usar codificação das acções faciais, ritmo cardíaco e alterações na retina ocular para determinar enganos", diz Nickerson, que usou o exemplo de sistemas de codificação de reconhecimento facial a serem usados em casinos em Las Vegas (EUA) para detectar batoteiros nas mesas ou para os manter fora do edifício por completo. "A lei em Vegas permite fotografar imagens genéricas de pessoas e usar a monitorização em tempo real nos casinos para essas ameaças", acrescenta.

Alguns especialistas argumentam que o reconhecimento facial tem um longo caminho a percorrer. Os que tentam passar despercebidos podem simplesmente baixar os seus chapéus ou cobrir os seus rostos, enquanto os sistemas de verificação podem ser facilmente enganados por uma imagem do rosto de uma pessoa.

Hauhn usa o exemplo de como a polícia na Flórida usou a videovigilância com reconhecimento facial de todos os que tinham mandados judiciais naquele estado, quando foi palco do evento desportivo Super Bowl há cerca de 10 anos. Ele salientou que havia milhares de falsos positivos, mas Nickerson sustenta que, apesar das falhas, a tecnologia está avançada o suficiente para ser fiável.

"Em termos de vigilância e monitorização de entradas, tem melhorado exponencialmente a quantidade de controlo e de precisão que temos", diz Nickerson. ■

ptempresas.pt

PT

PT Empresas

IMAGINE. É POSSÍVEL.

Imagine uma empresa que consegue reunir numa única marca o que é necessário para dar resposta às necessidades das grandes, médias e pequenas empresas, das instituições e dos profissionais. Imagine que essa marca reúne em si toda a tecnologia e know-how empresarial da PT e que por isso oferece as melhores, mais inovadoras e personalizadas soluções integradas de comunicação, tecnologias e sistemas de informação. Imagine que esta é a marca do seu parceiro. Com a PT Empresas, é possível.

Saiba mais em **ptempresas.pt**