O DIREITO À SEGURANÇA

Num mundo cada vez mais digital,
o papel da cibersegurança é cada vez mais essencial
para todos podermos confiar na internet

Quase todos os dias se ouve falar de ficheiros pirateados em muitas das empresas e organizações que nos pedem os dados, e mais e-mails e outras informações, que nunca deveriam ser divulgados, passam a estar disponíveis na internet. Isso faz com que muitos dos cidadãos comuns recebam sistematicamente mensagens de spam, comunicação comercial que não desejam, até pedidos de resgate individuais de contas de e-mail, algo que parece aterrador, mas cuja solução pode estar apenas à distância da eliminação do e-mail.

Numa altura em que começamos a ultrapassar uma crise sem precedentes, pelo menos desde que a democracia foi de novo implantada em Portugal, há 48 anos, faz todo o sentido abordarmos o tema da segurança, principalmente das pessoas e dos seus bens e serviços. E não só em relação ao que se compra através dos sites das empresas, sejam produtos ou serviços que têm de ser entregues com as características e qualidade prometidas, mas também no que diz que respeito ao sigilo dos dados de pessoas e empresas envolvidas nas trocas comerciais, que tem de ser garantido. Não podem nem devem ser partilhados, a não ser que os envolvidos aceitem fazê-lo.

SOLUÇÕES EFICIENTES PROCURAM-SE

Como é de Segurança que iremos falar neste especial da revista Exame Informática, procuramos explicar de que forma é que as empresas, que usam ou operam

REINO UNIDO ESTÁ A IMPLEMENTAR NOVAS MEDIDAS DE SEGURANÇA CIBERNÉTICA PARA TELEFONES, TABLETS, SMART TV, RASTREADORES DE FITNESS E OUTROS DISPOSITIVOS

no mercado através da internet, asseguram os nossos dados, o sigilo em relação às transações que fazemos com cada uma delas, que são efetuadas e entregam o que prometem a tempo e horas, pelo preço acordado, e com a qualidade percebida. Também procuramos falar de legislação, principalmente aquela que diz respeito à prevenção.

O Reino Unido já está a procurar implementar novas leis de segurança cibernética. Estão a ser discutidas no parlamento do país as destinadas a manter os telefones, tablets, smart TV, rastreadores de fitness e outros dispositivos protegidos dos cibercriminosos. São propostos novos requisitos de segurança cibernética, para fabricantes e comerciantes de tecnologias de consumo que se podem conectar à internet ou a outros dispositivos. De acordo com a nova lei, as senhas padrão que vêm programadas nos dispositivos digitais e constituem um alvo fácil para os cibercriminosos serão banidas. Para além disso, os fabricantes terão de passar a ser mais transparentes na sua comunicação com os clientes em relação ao período de tempo em que os produtos irão receber atualizações de segurança e terão de criar melhores sistemas de comunicação de relatórios sobre vulnerabilidades encontradas nos seus produtos. O não cumprimento das medidas pode resultar em multas de até 10 milhões de libras (cerca de 12 milhões de euros) ou 4% da faturação global da empresa. É apenas um passo, mas a segurança em relação a tudo que fazemos na internet, e que instituições e empresas que operam no mercado, e pedem os nossos dados pessoais, têm de garantir é, também, essencial.

A SEGURANÇA DOS DADOS É ESSENCIAL

A demonstração de que os efeitos de ataques de hackers podem ser devastadores para pessoas, empresas e instituições foi sentida recentemente em Portugal e amplamente divulgado na comunicação social. O ataque aos sites da Impresa, detentora da SIC e dos jornais Expresso e Blitz, deixou a empresa sem internet e destruiu muitos dos seus ficheiros, ainda não se sabe se para sempre. Mais recentemente um ataque cibernético teve como alvos sites do Governo da Ucrânia, e a Rússia desmantelou, por pressão dos Estados Unidos, o grupo de piratas informáticos REvil, "um dos mais temidos grupos de cibercriminosos em ransomware", segundo informação divulga pela Agência Lusa. Estes são apenas alguns exemplos do que também se passa nos dias de hoje com a democratização da internet, para além da facilidade de comunicação, do acesso à informação e da descentralização de serviços, ente outros.

Estar em segurança significa que se está ao abrigo de quaisquer perigos, danos ou riscos. Algo que é seguro é certo, correto, firme e estável, indubitável. Ou seja, a segurança é uma certeza. Por exemplo de que podemos atravessar o rio Tejo sobre a Ponte 25 de Abril, ou sobre qualquer outra em Portugal e no mundo, porque toda a sua estrutura é firme e estável, e dá-nos confiança. A mesma que temos nas leis que estabelecem limites ao comportamento dos seus cidadãos e à forma como agem, em sociedade e em termos gerais, num estado de direito. Têm de ser certas e corretas. Só assim podemos acreditar nelas.

Também temos como certa, ou quase, a segurança alimentar, aquela que nos garante a disponibilidade e o acesso a bens alimentares, com qualidade e em quantidade suficientes. Pelo menos em Portugal, dado que isso não acontece, como se sabe, em todos as partes de um mundo, pois ainda há milhares de pessoas a morrer diariamente de fome. A segurança alimentar apenas faz sentido a partir do momento em que se verifica que todas as pessoas têm, em qualquer instante, acesso físico e económico a alimentos para satisfazer as suas necessidades. A segurança é, sobretudo, um bem ao qual todos temos direito e é ao estado que compete defendê-la, em primeiro lugar, para assegurar, não só o bem-estar, como a qualidade vida dos cidadãos.

TAMBÉM NO UNIVERSO DIGITAL, ESTAR EM SEGURANÇA SIGNIFICA QUE SE ESTÁ AO ABRIGO DE QUAISQUER PERIGOS, DANOS OU RISCOS

A CIBERSEGURANÇA É ESSENCIAL PARA AS ORGANIZAÇÕES

No mundo cada vez mais digital, é fundamental que as empresas partam da premissa que serão atacadas um dia e desenvolvam uma cultura de ciberdefesa

Segundo Nuno Cândido, Cloud & Security Associate Director na Noesis, as empresas devem estabelecer programas internos de criação de uma verdadeira cultura de cibersegurança, numa lógica contínua e de longo prazo, optando por soluções que envolvam a Inteligência Artificial (IA). Para este responsável, "a cibersegurança tem de passar a fazer parte da cultura e do ADN das organizações".

Momentos de crise levam-nos a dar passos gigantes que nos ajudam no presente e trazem benefícios para o futuro. A crise causada pela pandemia de Covid-19 teve efeitos semelhantes no mercado da cibersegurança?

Devido ao efeito da pandemia causada pela Covid-19, a generalidade das organizações entrou em modo de sobrevivência e de reinvenção da forma como trabalham, das suas ofertas, dos seus modelos de negócio e da maneira como chegam aos seus clientes finais. Em paralelo houve uma hiperacelerarão da digitalização da economia, que trouxe novos desafios ao nível da segurança. O crescente desenvolvimento de ambientes multicloud ampliou a cyber-exposição, o número de pontos de falha e a vulnerabilidade das redes e ambientes, que os cibercriminosos têm sido rápidos a explorar sob as mais variadas formas. Por isso é fundamental que as organizações se voltem a focar na sua arquitetura de segurança. É necessário mudar o paradigma e adotar estratégias de reforço da confiança digital, que envolvam atributos como o risco, a conformidade regulamentar, a privacidade e a ética de negócio.

A mudança tem sido acompanhada pela evolução das soluções de cibersegurança. A introdução da Inteligência Artificial (IA) contribuiu para a criação de uma nova abordagem face às soluções tradicionais, já que as novas se focam na procura de comportamentos anómalos e análise de padrões, ao invés da busca de comportamento malicioso. Para além disso acrescentam capacidade de análise e superam os limites da capacidade humana. São também são uma resposta aos próprios ataques, cada vez mais complexos e sofisticados e que recorrem, também eles, à inteligência artificial. Poder analisar informações, e eventuais anomalias, sem a sobrecarga dos recursos humanos, é uma das perspetivas que a inteligência assistida permite alcançar. Com menor esforço passa a ser possível monitorizar, de forma completa, as redes, e atuar em tempo real sobre as ameaças externas ou internas que afetam as organizações.

Quais têm sido os principais problemas, em termos de cibersegurança, que a Noesis tem detetado nos mercados onde está ativa? Quais são as causas?

Só entre fevereiro e março de 2020, por exemplo, registou-se um aumento de 84% do número de incidentes de segurança reportados em Portugal. No total do ano, esse valor cresceu 150% face ao período anterior.

A aceleração digital tem contribuído para o aumento exponencial de ciberataques e é hoje materialmente impossível afirmar que uma empresa está 100% preparada e protegida. Um dos grandes problemas que se colocam hoje às organizações, em termos de cibersegurança, é a incapacidade das suas equipas de TI estarem atualizadas em relação a estes temas e de responderem às ameaças crescentes. Para além disso, nem todas as organizações têm a capacidade de criar equipas especializadas e há escassez de profissionais qualificados no mercado. Tudo isto tem contribuído para aumentar a vulnerabilidade das organizações. Mas, em simultâneo, está também a ser um motor de inovação no mercado, com os fornecedores e os fabricantes a procurarem desenvolver soluções que garantam segurança e, em simultâneo, otimizem a intervenção dos recursos humanos.

Nuno Cândido, Cloud & Security Associate Director na Noesis

Numa altura em que as empresas exigem, cada vez mais, o acesso instantâneo a aplicativos e dados, quais são as condicionantes principais ao desenvolvimento do teletrabalho por parte das empresas e das suas pessoas?

A adoção de teletrabalho veio dificultar a segurança da informação das empresas. Nos últimos dois anos, as organizações, com os seus escritórios fechados, viram-se obrigadas a adaptar os seus métodos, formas e espaços de trabalho, apostando fortemente na tecnologia e num modelo trabalho remoto, que veio para ficar.

Como muitos dos colaboradores seguiam modelos de trabalho presencial e estavam descontextualizados do mundo digital, a mudança para teletrabalho, devido à pandemia, obrigou-os a desafiarem-se para aprenderem a utilizar novas ferramentas e técnicas. Mas a implementação de soluções como o teletrabalho vai muito para além do agendamento das tarefas do dia-a-dia num chat, ou de uma reunião por videochamada. Inclui, também, medidas para manter as equipas envolvidas e em sintonia e disponibilizar, a cada um dos seus membros, todas as ferramentas necessárias para poderem ter um desempenho de excelência, desde serviços de armazenamento e gestão de dados confidenciais (clouds) e serviços de segurança informática (proteção anti-phishing), a aplicações capazes de criar um ambiente centralizado e integrado de partilha de informações.

Quais são as soluções para garantir que o universo digital não para e os dados de pessoas, instituições públicas e outras organizações, e empresas se mantém acessíveis e não são destruídos?

> AS ORGANIZAÇÕES PODEM E DEVEM REALIZAR SIMULAÇÕES DE ATAQUES, COMO OS DE PHISHING JUNTO DOS SEUS COLABORADORES

Vivemos tempos de forte aceleração digital, em que tudo e todos estão conectados e a partilha de dados é cada vez maior. Esta evolução, para além de facilitar o quotidiano das pessoas e o dia-a-dia das organizações, veio também aumentar a complexidade de sistemas, aplicações, redes e dispositivos e contribuir, em simultâneo, para a degradação da sua segurança. Por isso, é essencial que as organizações desenvolvam uma cultura de ciberdefesa, partindo da premissa de que um dia serão atacadas. Deve envolver todos, incluindo os seus CEO, e ter sempre foco no trabalho cooperativo entre a organização e os seus fornecedores de cloud e tecnologia. É necessário garantir capacidades de segurança discretas dos vendors e holísticas em relação à especificidade das arquiteturas de TI que permitam minimizar o risco e mitigar o impacto de ciberataques.

Em relação à tecnologia, as organizações estão a apostar cada vez mais na aplicação de procedimentos de backup & restore, de soluções de Endpoint Detection & Response (EDR) e de Mobile Device Management (MDM) e na implementação de Multi Factor Authentication (MFA). No entanto, a implementação de tecnologia, por si, não garante o aumento sustentado da resiliência em termos de segurança. Por isso, é importante construir um plano estratégico que defina transversalmente a governance, as responsabilidades, os processos e a tecnologia.

Em cibersegurança, a proteção é tão forte quanto o seu elo mais fraco, papel muitas vezes atribuído ao fator humano, pela dificuldade em definir ou aplicar medidas de segurança. Quais são as principais medidas a tomar para reduzir o risco do fator humano?

O phishing é uma ameaça bem presente, cada vez mais sofisticada e preocupante. É, por isso, importante que as organizações estejam cada vez mais atentas e preparadas para este tipo de ataques. Ao nível individual, é essencial a atenção redobrada dos colaboradores quando respondem a e-mails ou acedem a informação e fundamental definir alguns passos que ajudem as organizações e, consequentemente aos seus colaboradores, a reduzir o risco de ciberataques.

As organizações podem e devem realizar simulações de ataques, como os de phishing junto dos seus colaboradores, para avaliar o seu nível de preparação e de atenção em relação a possíveis ataques, e preparar todos para lidar o melhor possível com ameaças reais.

NÃO HÁ SETORES LIVRES DE RISCO

Com a generalização do trabalho remoto, as organizações têm de garantir, mais do que nunca, que as suas equipas trabalham em segurança, quer estejam no escritório ou em casa

Rui Duro, Country Manager Check Point Software Portugal

Para Rui Duro, Country Manager Check Point Software Portugal, o investimento em cibersegurança, mais do que um garante de segurança, é hoje uma necessidade em termos da relação custo/benefício.

Em menos de uma década, a segurança cibernética emergiu como um dos temas mais importantes para a economia global, com o crescimento de incidentes e ataques a empresas e instituições. Qual é a situação atual em Portugal?

Em Portugal, os números não são animadores. Temos dados que indicam que, em 2021, as organizações portuguesas foram atacadas 881 vezes por semana, em média, o que, em relação a 2020, representa um aumento de 81%. Os ataques são transversais a todos os setores económicos, pela simples razão de que os seus autores olham apenas à possibilidade de obter lucro

O setor da Educação/Investigação foi o mais visado a nível nacional no ano passado, com as instituições a registar uma média de 2480 ataques por semana. A Saúde, em segundo lugar, mais que duplicou o número de ataques sofridos desde 2020, com uma média de 2290 por semana. Em terceiro esteve a Administração Pública/Setor Militar, com uma média de 1116 ataques semanais, mais do dobro do ano anterior. Mais do que nunca, estes números devem relembrar as organizações nacionais de que não há setores livres de risco.

Numa economia e numa sociedade cada vez mais digital, qual poderá ser o papel da prevenção para evitar falhas e riscos e sustentar a segurança das redes e de quem as usa? O que está e ainda deverá ser feito em Portugal e no resto do mundo?

> A IMPLANTAÇÃO DE NOVAS TECNOLOGIAS DEVE SER RÁPIDA, SIMPLES E SEGURA

Prevenção é a palavra de ordem! Mais do que detetar a entrada de um malware, há que evitar que seja sequer possível penetrar as barreiras de segurança de um sistema de uma infraestrutura.
Em Portugal, durante uns tempos, havia a ideia de que a cibersegurança não era um tema tão prioritário, uma vez que os riscos não se aplicavam a nós por sermos um país pequeno. Agora, pelas piores razões, começamos lentamente a ver as empresas a mudar a sua atitude e a procurar ser proativas na luta contra o cibercrime, apesar de ainda haver um longo caminho a percorrer, especialmente entre as micro e pequenas empresas.
Em Portugal, a velocidade de evolução das ameaças e dos ciberataques ainda é superior à da proteção do ambiente das empresas, apesar dos progressos.
Neste cenário, há que mudar e priorizar a cibersegurança em toda a espinha dorsal das organizações, desde as equipas técnicas aos membros administrativos e decisores. Esta alteração inclui desde as práticas simples que devem pautar o dia-a-dia de trabalho, como não abrir links, anexos de e-mails desconhecidos ou fazer backups regulares dos dados, às decisões de gestão que têm um peso considerável na proteção da organização, como a implementação, ou não, de soluções de segurança, o tipo de dispositivos utilizados e a extensão da proteção ao trabalho remoto.

Quais são as principais soluções de cibersegurança da Check Point para o mercado nacional e o que é que asseguram?

O leque de soluções da Check Point é bastante alargado e destina-se à proteção de todos os possíveis vetores de ataque. A arquitetura de segurança Check Point Infinity é a mais completa do mercado e protege a infraestrutura de uma empresa em todas as redes, cloud, endpoints e mobile incluídos. A gestão é feita de forma consolidada e centralizada, o que garante mais eficácia e tira peso dos ombros dos administradores de TI.
A generalização do trabalho remoto é inevitável no mercado nacional. Mais do que nunca, as organizações têm de garantir que as suas equipas trabalham em segurança, quer estejam no escritório ou em casa.
A Check Point Harmony Connect é uma solução SASE (Secure Acess Service Edge) que protege o acesso remoto aos recursos da empresa, garantindo igualmente proteção contra malware, ataques de phishing e outros ataques sofisticados. A visibilidade unificada para as ameaças, a rápida implementação e fácil escalabilidade fazem da Harmony Connect uma solução bastante atrativa para as empresas.
Uma das grandes batalhas a travar em Portugal é contra o mito de que as soluções especializadas de cibersegurança representam ainda um investimento incomportável para as empresas, especialmente micro e pequenas empresas. Na Check Point temos soluções ajustadas à dimensão e orçamento de cada organização.
Os ciberataques são, hoje, cada vez mais devastadores, corrompendo o funcionamento das empresas e obrigando, muitas vezes, a períodos de inatividade, com prejuízos significativos a nível financeiro. Em termos de custo/benefício, o investimento em cibersegurança, mais do que um garante de segurança, é hoje uma necessidade.

Numa época de mudança, as empresas precisam de sistemas que tornem a implantação de novas tecnologias e serviços, segura e simples? Quais são as vantagens?

À segurança e simplicidade, acrescentaria rapidez. Penso que estas são as características mais importantes para um empresário que pretende um sistema de segurança robusto para a sua organização. Acima de tudo, são necessárias soluções que se adequem ao modus operandi da empresa e garantam segurança ao longo de toda a infraestrutura e vetores de ataque, sem que seja necessário proceder a alterações estruturais.
Para além do que referi há pouco sobre a importância de a cibersegurança acompanhar o ritmo do cibercrime, garantir que a transição para um ambiente de trabalho mais seguro decorre sem fricção é uma forma de encurtar distâncias.

A cibersegurança deverá hoje ser também uma preocupação dos gestores de topo? Quais são os benefícios, para as organizações, do seu maior envolvimento nesta área?

Definitivamente. Ao fim ao cabo, quem toma as decisões de investimento são os gestores no topo da hierarquia e é a eles que cabe orientar as suas equipas. A cibersegurança deve fazer parte dos princípios-base das empresas e deixar de ser um tema secundário. Os benefícios são claros: maior proteção, maior tranquilidade e maior liberdade no trabalho remoto.

OS SISTEMAS DE INFORMAÇÃO ESTÃO CADA VEZ MAIS EXPOSTOS A CIBERATAQUES

É essencial assegurar níveis elevados de proteção, e celeridade e eficiência na resposta aos incidentes para garantir a segurança das organizações

Pedro Morais, Founding Partner da NextBITT, diz que a sua empresa desenvolve um trabalho que lhe permite ter uma evolução permanente na área da cibersegurança. Inclui a adoção das tecnologias mais recentes e a melhoria contínua dos procedimentos.

Agora que começamos a ultrapassar uma crise sem precedentes, tem havido notícias de ataques informáticos crescentes a pessoas, empresas e instituições, com efeitos mais ou menos intensos. Quais são os principais problemas que a NextBITT tem detetado atualmente?

Com a deslocalização dos colaboradores das empresas e o aumento tendencial do teletrabalho, a interpretação de perímetro de segurança das organizações mudou radicalmente.

Durante a pandemia, as empresas tiveram de adotar novos procedimentos e novas tecnologias de segurança, que lhes permitissem fazer face à movimentação dos postos de trabalho dos escritórios para casa e ao aumento do número de ciberataques.

Com a Transformação Digital, processo que tem acelerado muito nos últimos anos, os sistemas de informação estão cada vez mais expostos a este tipo de ataques.

A cultura das organizações em temas de cibersegurança está a evoluir. No entanto é essencial, não esquecer que o trabalho necessário para garantir níveis elevados de proteção, e celeridade e eficiência na resposta aos incidentes, é intenso e permanente.

O que é que ainda pode ser feito mais para impedir, ou pelo menos diminuir os efeitos de ataques cibernéticos a empresas e outras instituições? A legislação atual é a mais adequada?

No âmbito da prevenção e da mitigação do efeito dos ataques, salienta-se a necessidade de as organizações terem equipas ou parceiros especializados em cibersegurança, para implementarem tecnologias e procedimentos de segurança. Para além disso, também precisam de sensibilizar as suas pessoas para este tema e para o risco que as empresas podem correr com as suas ações, e preparar as suas equipas em treino defensivo e ofensivo.

Pedro Morais, Founding Partner da NextBITT

> A NEXTBITT É UMA TECNOLÓGICA QUE OFERECE SOLUÇÕES ENTERPRISE PARA AS ÁREAS DE ASSET, FACILITY MANAGEMENT & SUSTAINABILITY, DIRECIONADAS PARA AS GRANDES ORGANIZAÇÕES

Com o aumento da exposição aos riscos crescentes, e as alterações mais recentes dos quadros legais, contidas no Decreto-Lei n.º 65/2021, que regulamenta o regime jurídico da segurança do ciberespaço, as organizações têm, hoje, mais obrigações na área da segurança relacionadas com temas de certificações de cibersegurança.

Com a evolução crescente do trabalho remoto e a necessidade do desenvolvimento de novas tecnologias para o sustentar, a evolução da digitalização está a crescer de uma forma sem precedentes. Também tem sido impulsionada, por exemplo, pela necessidade de criação de tecnologias que sustentem a evolução do atual modelo energético global para outro mais sustentável. Como é que se assegura a evolução deste mundo em mudança? Quais são os princípios essenciais a seguir?

A NextBITT é uma tecnológica que oferece soluções *enterprise* para as áreas de Asset, Facility Management & Sustainability, direcionadas para as grandes organizações. Como aposta estratégica, a NextBITT está a investir em soluções que visam dar resposta às preocupações de sustentabilidade suportadas nos módulos de SGE (Sistema de Gestão Energética) e SGA (Sistema de Gestão Ambiental) e na mudança do trabalho presencial para o teletrabalho, que cresceu exponencialmente devido à pandemia e tende a manter-se nos dias de hoje.

> O USO DAS MELHORES PRÁTICAS PERMITE, À NEXTBITT, GARANTIR, AOS CLIENTES E PARCEIROS, O USO DE CRITÉRIOS RIGOROSOS DE SEGURANÇA

A segurança é, sobretudo, um bem ao qual todos temos direito. A que empresas como a NextBITT oferecem em relação à atividade que desenvolvem é, também, essencial. Como e onde a empresa desenvolve o seu trabalho e o que garante?

A NextBITT é uma empresa *born-in-the-cloud*. Toda a sua oferta e a forma de operar é baseada em cloud. Os nossos produtos são desenvolvidos com tecnologias Microsoft e distribuídos na Cloud Microsoft Azure.

O uso das melhores práticas de segurança do mercado permite-nos garantir, aos nossos clientes e parceiros, critérios rigorosos de segurança, já que as nossas equipas adotam sempre procedimentos de segurança *Zero Trust*, quer estejam a desenvolver o seu trabalho em perímetros mais controlados ou em teletrabalho.

Quais são as novidades da empresa previstas até ao final deste ano?

A NextBITT desenvolve um trabalho que lhe permite ter uma evolução contínua na área da cibersegurança, com a adoção das tecnologias mais recentes, que nos garantem os máximos critérios de segurança e, também, a melhoria contínua dos nossos procedimentos.

Para 2022, queremos dar mais um passo estratégico. Por isso, estamos a preparar o processo para que a NextBITT seja certificada pela norma ISO27001. É um referencial internacional da Segurança de Informação e estabelece um padrão e um código de boas práticas relativas à gestão de Segurança de Informação.

OPINIÃO

VÍTOR VENTURA **, MANAGER EMEA & ASIA, CISCO TALOS OUTREACH**

É URGENTE NORMALIZAR OS CIBERATAQUES

É importante não sobrevalorizar os seus impactos, origens ou motivações, sob pena de perderem a sua real relevância

É urgente normalizar os ciberataques. O pedido pode parecer contraditório, mas a ação é realmente necessária e indispensável.

Portugal tem de passar a encarar estes eventos com a mesma naturalidade com que observa um acidente de viação. Ambos são indesejados, eventualmente até graves, mas fazem parte do quotidiano das sociedades modernas. Sofrer um ciberataque não é um sinal de fraqueza. É, apenas, algo que, neste momento, pode acontecer a qualquer pessoa ou organização.

Não se pretende, com isto, desvalorizar os incidentes de segurança no ciberespaço. Mas é importante também não sobrevalorizar os seus impactos, origens ou motivações, sob pena de estes perderem a sua real relevância, abrindo espaço ao aproveitamento populista e especulativo.

Quando pensamos em cibersegurança temos de ter em conta três intervenientes diferentes: pessoas, organizações e governos. Embora sejam complementares, as interações entre eles podem ser vistas de um ponto de vista piramidal, onde cada um tem as suas responsabilidades e preocupações.

No topo da pirâmide estão as pessoas. Ao longo do tempo, o utilizador foi sendo retratado como o "elo mais fraco" da cibersegurança, por abrir anexos em emails ou fornecer as suas credenciais em páginas de autenticação falsas. É, por isso, importante formar as pessoas para que tenham uma maior consciência para a segurança na Internet.

A curiosidade e o erro são características sobejamente conhecidas de quem é humano. Daí que caiba às organizações, públicas ou privadas, dotarem-se dos meios necessários para aumentarem a sua resiliência no ciberespaço. Ou seja, de se capacitarem para resistir e, se necessário, operar e recuperar de um ciberataque, com o mínimo de impacto possível no negócio.

Se as organizações tiverem sistemas de autenticação com múltiplos fatores, por exemplo, um atacante não poderá utilizar as credenciais obtidas de um utilizador incauto. Outro exemplo será a criação de um plano de resposta a incidentes de cibersegurança, que possibilita um regresso mais rápido ao "estado normal", sem que se sacrifique a investigação ou exista o risco de reincidência.

Ao Estado cabe a investigação e punição dos responsáveis, que têm de ser castigados apesar de serem responsáveis por causar algo que é comum.

Os governos têm um papel único na normalização dos ciberataques, por via de uma maior transparência. É aceitável que, durante um ataque, não se divulguem detalhes. Mas, a longo prazo, essa falta de visibilidade torna-se prejudicial para uma sociedade que se quer dotada de literacia digital. A opacidade só contribui para um clima elitista e de secretismo, que não é compatível com a tal normalização que se pretende. Por isso é fundamental explicar os incidentes de cibersegurança com termos que todos possam entender.

Todos nós somos utilizadores do ciberespaço, seja no telemóvel ou no computador, na televisão ou no tablet. A clarificação de tudo o que diz respeito aos ciberataques, e a sua normalização, aumentam a resistência dos utilizadores e limitam a especulação e o eventual aproveitamento populista. As organizações já fomentam a literacia digital através das suas formações internas. Ao Estado cabe o papel mais abrangente: o de formar a sociedade em geral.

OPINIÃO

DIOGO PATA
GLOBAL SALES ENGINEER, WATCHGUARD

A IMPORTÂNCIA DA SEGURANÇA NAS ASSINATURAS ELETRÓNICAS E DIGITAIS

Sem as medidas de segurança adequadas, as assinaturas digitais usadas nas empresas e na administração pública podem ser-se uma porta de entrada para cibercriminosos

As assinaturas digitais são usadas cada vez mais nas empresas e na administração pública. No entanto, sem as medidas de cibersegurança adequadas, este método pode ser um vetor para cibercriminosos e autores de fraudes. Através de engenharia social, podem levar as vítimas a acreditar que um documento é legítimo e, através da sua assinatura, obter autorização para realizar outras operações sem consentimento, entre muitas outras atividades maliciosas.

Existem algumas formas de evitar isto. Mas, primeiro, é necessário distinguir os conceitos de assinatura eletrónica ou e-assinatura e de assinatura digital, até porque a cibersegurança desempenha um papel chave nesta diferenciação. Embora muitos media e fontes usem estes termos alternadamente, na verdade todas as assinaturas digitais são eletrónicas. Mas nem todas as assinaturas eletrónicas são digitais.

Na teoria, o propósito de uma e-assinatura é validar a autenticidade de um documento. Mas as assinaturas digitais vão mais além, porque são um tipo específico de assinatura eletrónica que providencia uma segurança adicional. Além de assegurarem a autenticidade de um documento, as assinaturas digitais empregam métodos de criptografia, como certificados digitais (por exemplo, SSL), para garantir que terceiros não interferem no processo. Porém, para uma maior garantia de segurança de que os signatários são legítimos e já estão incorporados em certificados de assinaturas digitais (DSC, na sigla original), com um certo nível de cibersegurança, deve ser também implementada alguma forma de autenticação multifatorial (MFA).

Os certificados de assinaturas digitais estão divididos em três categorias: Classe 1 (DSC1), Classe 2 (DSC2) e Classe 3 (DSC3). A primeira representa um nível básico de segurança, porque a validação é feita por email e/ou password. Não é adequada para ser usada em documentos legais e só é válida para documentos e ambientes de risco muito reduzido. Os de Classe 2 (DSC2) são os certificados mais comuns da assinatura de documentos. Verificam a autenticidade do signatário em relação a uma base de dados pré-estabelecida e incluem um segundo nível de verificação, para garantir que a assinatura é a original do registo. O nível de segurança mais elevado, DSC3, é, também, o menos prático, pois requer uma organização ou terceiros para verificar a identidade do signatário antes da assinatura. Por esta razão, a sua utilização tende a restringir-se a documentos legais, onde as consequências de uma falha de segurança podem ser muito perigosas.

Para a grande maioria dos documentos das organizações, o certificado DSC2 deverá ser suficiente, porque os processos que requerem certificações DSC3 são geralmente demasiado dispendiosos em termos de recursos e de tempo.

No entanto, é imperativo que os certificados DSC2 incluam um método de verificação adicional.

Tenha, em mente, que 61% das falhas de segurança envolvem credenciais das vítimas. Se os cibercriminosos têm acesso a essas credenciais, podem usar um certificado digital obtido previamente. Mas se uma organização tiver um segundo método de verificação, como um serviço de autenticação multifatorial (MFA), fácil de gerir e altamente seguro, reduzirá significativamente as hipóteses de os documentos serem manipulados. Neste sentido, as soluções mais avançadas têm, inclusive, proteção MFA adicional nos telemóveis, para garantir que são os dispositivos autorizados e, assim, impedir que os atacantes possam utilizar telemóveis clonados.

OPINIÃO

JOÃO LOPES MANSO
CEO DA REDSHIFT

POR ONDE ANDAM OS NOSSOS DADOS?

Para assegurar que os dados estão menos desprotegidos, é preciso garantir o respeito pelas leis relativas à cibersegurança

Nas últimas semanas temos assistido a uma série de ciberataques em Portugal, que afetaram entidades tão distintas como operadores de telecomunicações, empresas da saúde, meios de comunicação social e até um órgão de soberania. Claro que estou a referir apenas aos que se tornaram, inevitavelmente, públicos.

Públicos, porque a maioria não sente a necessidade de declarar nada. E ainda temos todos os outros, aqueles cujos responsáveis nem fazem ideia de algo se ter passado.

Uma coisa parece óbvia, contrariamente ao que se passa no resto do mundo, os nossos dados pessoais, confiados às instituições públicas estão seguros, pois destas não existem notícias de ataques nos últimos tempos.

Em relação à maioria dos mais recentes acontecimentos, salienta-se que todos os responsáveis declararam rapidamente "que não foram acedidos dados", "o ataque não foi direccionado a dados" ou "não existem evidências de ter existido acesso a dados". E todos nós tendemos a pensar que somos um país genial, em que as equipas de protecção de dados são muito superiores às de cibersegurança, pois os sistemas são atacados, mas os dados mantêm-se a salvo. Como não temos reporte ou estatísticas de violações por parte da Comissão Nacional de Proteção de Dados (CNPD), temos que acreditar que os nossos continuam seguros.

É claro que nem todos os ataques têm como objectivo os nossos dados, porque nem todos têm fins lucrativos (da venda dos dados). Mas o que se vem notando é que, pouco após os ataques, aparecem indícios da existência de vendedores da informação recolhida ou existe partilha efectiva da informação obtida, acedida, desviada ou roubada, vá-se lá saber como... Existem outros, que alguém definiu como "ataques à nossa memória", que procuram destruir informação arquivada. Mas também estes são violações, pois impossibilitam-nos de saber o que existia e, existindo, quem teve acesso.

A lei da protecção de dados exige medidas técnicas como "cifragem", "confidencialidade, integridade, disponibilidade e resiliência permanentes", e para "restabelecer a disponibilidade e o acesso ... de forma atempada" e "testar, apreciar e avaliar regularmente". Mas o que constatamos, com base nos incidentes mais recentes, é que algumas destas regras não estão implementadas, ou estão mal implementadas, mesmo após avisos e exemplos e "continuados investimentos" em cibersegurança, como nos garantem os responsáveis das "vítimas".

Para quem observa por dentro, a realidade é outra. Os investimentos são reduzidos e pouco abrangentes, seja por restrição de investimento, ou pior, por falta de visão e de sentido de responsabilidade da liderança. Vemos empresas e entidades governamentais, que gastam milhões em novos sistemas e soluções comerciais, mas mantêm soluções absolutamente arcaicas e obsoletas de segurança, com recurso a processos manuais, porque acham que gastar umas dezenas de milhar em segurança é um exagero sem retorno.

Coisas básicas como, por exemplo, a identificação e mitigação de vulnerabilidades nas infra-estruturas e aplicações, em muitas destas "vítimas", são feitas quando são, de forma esporádica e manual, sem prioridade, fora de prazo. Isto também acontece em empresas e entidades responsáveis por serviços essenciais e infraestruturas críticas.

Temos que ser nós a exigir saber o que se passa, e o que é feito. Se não o fizermos, o que podemos ter a certeza é que "no pasa nada". Muito falta fazer, principalmente em respeito pelas leis existentes, mas também pela ética, transparência e consideração por quem disponibiliza informação para empresas e as entidades do estado nos prestem serviços, e cobrarem por eles. Faltam-nos, principalmente, políticos e elementos do governo sinceramente preocupados com a cibersegurança, para que os nossos dados possam ficar um pouco menos desprotegidos.

Termino com o que foi afirmado por um político em directo na televisão, esta semana: "Ainda bem que não se lembraram de atacar outros alvos. Se não precisávamos de ajuda europeia".

OPINIÃO

ARNALDO COSTEIRA
DIRETOR-GERAL DE COMUNICAÇÃO E RELAÇÕES EXTERNAS DO ISEC LISBOA
DOCENTE UNIVERSITÁRIO

CASA ARROMBADA...

A cada minuto que passa são gerados, em todo o mundo, mais de 1,5 mil terabytes de dados, um verdadeiro tsunami de informação que se agiganta à razão de mais de 40 trilhões de gigabytes de dados por ano. Grande parte dessa informação é sobre nós! São os nossos dados pessoais, informação classificada e sensível sobre os nossos comportamentos e consumos, são as nossas empresas e instituições virtualizadas a que acedem mais de 6 bilhões de dispositivos (smartphones e computadores).

Falar em segurança da informação é considerar esta área de exposição praticamente ilimitada, em que o risco à privacidade dos nossos dados é tanto maior quanto maior é o número de dispositivos que usamos no acesso a informação sensível.
Há uma ideia errada de que a cibersegurança é problema exclusivo das empresas, mas temos que ter consciência de que todos contribuímos a cada instante, com os nossos dados pessoais, hábitos e interesses, partilhados em plataformas de compras, entretenimento, informação e ensino.
O RGPD trouxe enormes desafios às organizações na garantia da privacidade dos dados pessoais, mas a dependência crescente das redes sociais, do armazenamento de dados na cloud e do recurso a SaaS e a servidores remotos, trouxe-nos a um patamar em que o controlo da informação já não está na dependência do seu titular.
A pandemia ampliou o risco, pela iliteracia digital e pelo aumento de acessos remotos à informação empresarial.
O objetivo deste artigo de opinião é o de trazer uma reflexão sobre os níveis de alerta e atenção que devemos ter, enquanto decisores nas nossas instituições, para os sistemas de segurança e controlo no acesso à informação que produzimos e dos dados pessoais com que estamos comprometidos em garantir a privacidade.
Organismos como o CNCS, que lidera o esforço de sensibilização dos cidadãos e das empresas para as boas práticas no acesso e gestão da informação e de comportamentos a adotar enquanto utilizadores da Internet, abrem caminho à literacia digital redutora das ameaças do cibercrime, mas cabe-nos a nós, todos, o dever de buscar o conhecimento e desenvolver competências que nos permitam adotar comportamentos e sistemas de controlo e segurança, para estarmos melhor preparados para as ameaças e ataques cada vez mais sofisticados.
Casos como o da Vodafone ao nível da cibersegurança, ou da Câmara Municipal de Lisboa ao nível da proteção de dados, são exemplos de que o risco e a falha são uma questão de tempo.
Não podemos continuar na expectativa de 'se' pode acontecer, mas na certeza de que, sendo uma inevitabilidade, devemos estar preparados para 'quando' acontecer.
A formação e a capacitação de todos quantos têm em mãos a gestão de dados e da segurança de informação é fundamental a este esforço coletivo que temos que fazer, em linha com a estratégia nacional de cibersegurança e da proteção de dados. A nós no CESICP, e no ISEC Lisboa enquanto instituição de ensino superior, compete-nos fazer a nossa parte, disponibilizando as ferramentas e conhecimentos potenciadores deste saber-fazer. E é o que fazemos.