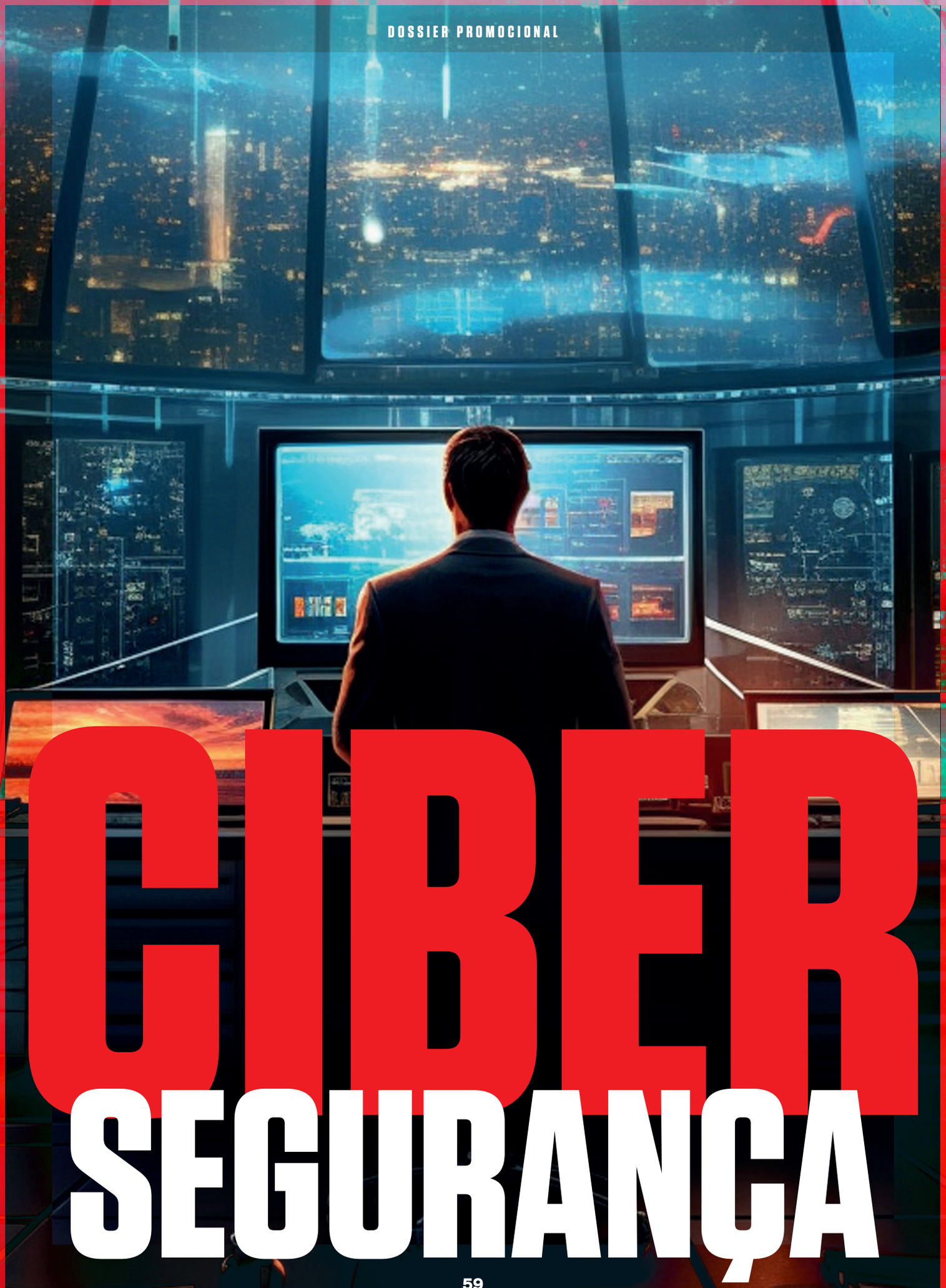


CIBER SEGURANÇA

CIBERSEGURANÇA DEVE SER UMA COMMODITIE NAS EMPRESAS

Proteger os sistemas digitais é uma necessidade e um investimento que terá retorno imediato. Prevenir, antecipar, mitigar e recuperar são requisitos essenciais para uma abordagem completa da segurança nas organizações. Regulação mais exigente contribui para aceleração na adoção destas ferramentas

Os últimos anos reforçaram a importância da cibersegurança nas empresas, mas também no setor público. Uma constante 'corrida de gato e rato' entre cibercriminosos e profissionais da segurança tem dinamizado uma área a que muitos não davam a devida atenção, e ajudou a desfazer o mito de que apenas as grandes empresas são alvo de quem procura obter ganhos financeiros ou satisfazer outros propósitos como, por exemplo, a desinformação ou a guerra cibernética entre Estados.

Neste contexto, os ciberataques relacionados com os conflitos internacionais e a ciberguerra são uma tendência crescente desde o início da guerra na Ucrânia, reforçado mais recentemente pelo conflito entre Israel e Gaza. Neste tipo de ameaças, o objetivo passa por atacar serviços e infraestruturas públicas, mas também empresas privadas, com vista a provocar instabilidade e impacto económico. Muitos dos grupos que atuam com este propósito são mesmo financiados por governos, como é o caso da China, da Rússia, do Irão ou da Coreia do Norte.

Mas, neste tipo de cibercrime, outro objetivo é também a desinformação que ajuda a criar instabilidade social e política. Com muitos países do mundo – nomeadamente os Estados Unidos – a ter, em 2024, eleições cujo impacto se reflete a nível global, os riscos crescem ainda mais. Para os especialistas do Fórum Económico Mundial (FEM), as organizações devem estar alerta não só às ameaças mais comuns, mas também a possíveis campanhas de desinformação através das redes sociais. Áudios e vídeos ou outro tipo de imagens falsos gerados com Inteligência Artificial (IA), os chamados 'deepfake', serão mais frequentes e tão realistas que podem enganar até os mais atentos.

É precisamente a massificação de tecnologias emergentes como a IA que está igualmente a provocar uma ainda maior aceleração no desenvolvimento de soluções de cibersegurança, exigindo um maior cuidado na sua gestão por parte das organizações. No entanto, como alerta FEM, é preciso estar atento às ameaças que a IA pode colocar às empresas e à sociedade. Segundo o relatório global sobre cibersegurança para 2024, o FEM aponta o risco crescente inerente à rápida massificação da IA generativa e de outras tecnologias que podem ser facilmente utilizadas em ciberataques. A instituição, que tem por objetivo contribuir para a construção de um mundo melhor, política e economicamente, recomenda que as organizações consigam manter um equilíbrio entre a necessidade de utilizar estas tecnologias ao serviço dos seus negócios e os riscos que podem causar.

IA AJUDA A DEFENDER, MAS ENSINA A ATACAR

Com o recurso à IA generativa e a ferramentas de machine learning, os especialistas em cibersegurança conseguem desenvolver soluções mais "inteligentes" e sofisticadas, mais rapidamente, e colocá-las no mercado, ao serviço das empresas. Contudo, a facilidade com que estes especialistas criam ferramentas com maior capacidade de defesa, tem um paralelo do lado do 'inimigo'. Ou seja, também os cibercriminosos estão a tirar partido do mesmo tipo de ferramentas que, graças à velocidade de aprendizagem, lhes permite atacar com maior frequência, mais rapidamente, e com maior sucesso. Exemplo disso é o aumento significativo nos ataques de engenharia social, mais difíceis de detetar, quer pelos sistemas, quer pelos utilizadores. Exemplo disso são mensagens de phishing por WhatsApp ou através de outras redes sociais, cada vez mais frequentes e personalizadas, ou o código malicioso que permite criar deep fakes (imagens e áudio que não correspondem à realidade).

No entanto, à margem da velocidade a que surgem novas soluções de defesa, e artimanhas de ataque, a verdade é que o investimento em cibersegurança não pode ser descurado pelas organizações que têm que estar preparadas para esta luta permanente. Não estar atento significa que, mais tarde ou mais cedo, terá um prejuízo avultado para recuperar de um ataque sendo que este é tanto mais elevado quanto maior for a demora em detetá-lo. Em média, um ciberataque pode demorar entre 250 e 750 dias a ser detetado, de acordo com estudos desenvolvidos por diferentes entidades. Isto significa que quando o ataque é detetado, a empresa já perdeu milhares de euros entre os prejuízos da quebra de segurança, o roubo de dados, ou os danos que o cibercrime deixa nos seus sistemas.

Em Portugal, e apesar do longo caminho a percorrer, investir em cibersegurança é atualmente uma prioridade para grande parte das organizações. A conclusão é do estudo "O estado da cibersegurança em Portugal", desenvolvido pela Microsoft, que

revela que 45% das empresas preveem investir na segurança digital este ano. Adicionalmente, o estudo revela que 84% dos inquiridos acredita que este investimento deve começar pela consciencialização dos colaboradores sobre o tema.

Chegada a hora de investir, revela a mesma pesquisa, a maioria dos inquiridos (41%) assume que o investimento ficará abaixo dos 10.000€, 20% baliza o investimento entre 10.000€ e 50.000€, enquanto uma percentagem considerável (35%) desconhece os investimentos previstos. Um cenário que reforça alguma indefinição estratégica do lado das organizações, e que permite concluir que, em geral, o grau de maturidade e de práticas de cibersegurança nas empresas ainda não é muito elevado.

Questionadas sobre o retorno do investimento, as empresas que responderam a este estudo e que já investiram na implementação de medidas de segurança cibernética, asseguram que o esforço financeiro compensou e que é facilmente mensurável. Em geral, estes inquiridos revelam que a sua organização teve menor exposição a incidentes e menos casos associados a perda de dados e a danos financeiros.

REGULAÇÃO EUROPEIA APONTA O CAMINHO

O contexto de guerra física que se vive na Europa e no Médio Oriente acelerou a necessidade de reforçar a proteção das empresas e das sociedades, mas também da regulação. A nível mundial, foram publicadas várias diretivas de cibersegurança, quer nos Estados Unidos – com o regulamento definido pela Comissão de Segurança e Proteção, SEC –, quer na Europa, com a diretiva NIS2, que será obrigatória a partir de 2024.

O objetivo destas 'regras' passa por responsabilizar as empresas que terão obrigatoriamente que adotar medidas de prevenção de ciberameaças, garantindo que estão protegidas e capacitadas para minimizar o impacto de eventuais incidentes cibernéticos, e que notificam as autoridades competentes caso ocorram. Os destinatários da nova regulação são PME e grandes empresas, especialmente de setores críticos, como administração pública, infraestruturas digitais, saúde, banca, finanças, transportes ou energia. Recorde-se que, em 2023, uma em cada oito empresas foi alvo de um ataque que resultou em prejuízos muito avultados e que, em média, cada organização sofre 89 tentativas diárias de intrusão nos seus sistemas.

EM QUE INVESTIRAM AS EMPRESAS EM PORTUGAL

81%
ANTIVÍRUS E MALWARE

71%
MEDIDAS DE AUTENTICAÇÃO FORTES PARA O ACESSO A SISTEMAS CRÍTICOS

37%
FIREWALLS E AUTENTICAÇÃO MULTI-FACTOR

36%
CRIPTOGRAFIA DE DADOS, PARA PROTEGER OS ATIVOS DA EMPRESA

FONTE: ESTUDO DA CIBERSEGURANÇA EM PORTUGAL, MICROSOFT

CENÁRIO DE AMEAÇÃS DE RISCO CIBERNÉTICO

FONTE: COVEWARE

Mas, apesar de serem cada vez mais as empresas que, em Portugal, olham para a cibersegurança como um investimento obrigatório, o cenário é bastante distinto quando se procura quantificar a conformidade do setor empresarial com a Diretiva NIS – que procura uniformizar a resiliência do espaço europeu de cibersegurança –, incluída na estratégia europeia para a segurança digital. Esta diretiva foi adotada em 2016, e transposta para a legislação portuguesa em 2018, será, a partir de 2024, substituída por uma nova diretiva – a NIS2.

O Centro Nacional de Cibersegurança (CNCS) é, desde então, a entidade responsável pela supervisão da adequada implementação da Diretiva NIS, enquanto sobre as entidades recai a obrigação de cumprir – com requisitos de segurança da informação e Instruções do CNCS – e de notificar – incidentes de segurança relevantes. Cabe igualmente a esta instituição divulgar as regras associadas a esta diretiva, procurando levar junto das empresas toda a informação de que necessitem para agir em conformidade.

Em 2022, o CNCS realizou um roadshow de norte a sul do país, mas reconheceu recentemente que esta iniciativa não deu os frutos esperados. Mais recentemente, adotou uma postura mais efetiva, tendo notificado cerca de 400 entidades, apesar de não serem conhecidas sanções que tenham sido aplicadas no contexto da Diretiva NIS em Portugal. Segundo o estudo "O estado da cibersegurança em Portugal", o setor empresarial nacional ainda demonstra muitas indefinições estratégicas e possíveis lacunas do ponto de vista de comunicação no que se refere à conformidade com a nova diretiva NIS2.

O DESAFIO DO TALENTO

O desenvolvimento do mercado da cibersegurança implica também um crescimento dos recursos especializados. Contudo, as universidades e o mercado não estão a conseguir dar resposta às necessidades, pelo que a guerra pelo talento é um dos grandes desafios atuais para os gestores e para as organizações. No setor público, o problema agrava-se, uma vez que os salários praticados não são atrativos. E este não é um problema apenas de Portugal, mas transversal a outros países da Europa e do mundo.

Sem possibilidade de formar novos especialistas à velocidade necessária, muitas organizações de maior dimensão estão a apostar na reconversão dos seus colaboradores, dando-lhes as competências necessárias aos desafios que enfrentam. Por outro lado, esta requalificação começa a ter eco do lado público, com o governo a disponibilizar um conjunto de programas e de ferramentas que contribuam para a adequação das competências. Mesmo profissionais de outras áreas estão a ser requalificados, como acontece, por exemplo, através do programa UpSkill. Neste caso, um conjunto de empresas candidata-se a receber novos recursos e partilha com os politécnicos e universidades parceiras do programa quais as suas necessidades em termos de competências. Estas instituições ficam responsáveis por toda a formação teórica dos candidatos, que depois recebem formação 'on the job'. As empresas que os recebem comprometem-se a pagar salários compatíveis com a função e a integrar os recursos num determinado período.

Atrair mais mulheres para as áreas tecnológicas é outro esforço que tem sido feito para conseguir mais profissionais especializados. Este número é hoje muito superior ao de há cinco ou dez anos, mas ainda há muito para fazer. Recorde-se que as mulheres representam cerca de 50% da população mundial, e que ocupam 40% das profissões altamente qualificadas. No entanto, no setor das TIC (Tecnologias de Informação e Comunicação) são apenas aproximadamente 24% da força de trabalho. De acordo com um relatório do Eurostat Portugal está, a este nível, acima da média da União Europeia, tendo crescido 6,5% nos últimos dois anos.

Recentemente, no dia 25 de abril, comemorou-se o Dia Mundial das Raparigas e Mulheres nas TIC, uma data que anualmente procura sensibilizar o mundo para este tema, e aproximar as jovens desta área profissional. Mas, é preciso fazer mais e, apontam diferentes estudos, a solução passa por criar programas que, desde o ensino básico, permitam informar e despertar o interesse por estas áreas, mas também bolsas de estudo para dinamizar a procura. ■

O Fortinet Security Fabric é a plataforma Mesh de cibersegurança com o mais alto desempenho do setor. Suportado por um amplo ecossistema, e alavancando automatização e facilidade de integração, disponibiliza extensas capacidades de cibersegurança tornando as arquitecturas mesh uma realidade. Permite acelerar os processos de transformação digital enquadrado por um contexto forte de cibersegurança, reduzindo a complexidade, simplificando a operação e aumentando as capacidades de deteção e resposta a ameaças. **Saiba mais em fortinet.com**

FORTINET

Copyright © 2024 Fortinet, Inc. All Rights Reserved.

PORTUGAL É UM HUB CENTRAL NO NEGÓCIO GLOBAL DA SIEMENS

A partir de terras lusas, a tecnológica que, no próximo ano, celebra 120 anos de presença em território nacional investiga e desenvolve um conjunto de ferramentas que suportam as tecnologias com que apoia as organizações na transformação digital. Subjacente a todas está a cibersegurança, área que a multinacional alemã endereça de forma holística e baseada em dados, que inclui a segurança dos produtos, dos sistemas e das operações

Em entrevista à *Exame Informática*, Luís Costa, especialista em Cibersegurança na Siemens Portugal, explica a forma como a empresa olha e endereça a cibersegurança, um dos seus pilares estratégicos. O responsável fala ainda sobre o caminho seguido pela multinacional com o objetivo de tornar o mundo digital mais seguro, e a sua participação na aliança Charter of Trust, bem como sobre a importância da equipa do Lisbon Tech Hub na estratégia global da Siemens.

A Siemens é hoje uma referência na cibersegurança, nomeadamente, nas soluções que disponibiliza para a indústria. Que ligação tem a empresa a esta área e porque é importante?
A Siemens liga os mundos real e digital como nenhuma outra empresa, e cria tecnologias que capacitam os seus clientes a transformar as indústrias em que operam, e que são cruciais para qualquer economia, como as infraestruturas, a energia, a indústria, a mobilidade ou a saúde. A empresa quer contribuir ativamente para os planos de descarbonização e transformação digital dos seus clientes e do país, criando impacto na sociedade através da sua tecnologia. O foco na cibersegurança permitirá gerar a confiança necessária para que estas transições, que tanto ambicionamos, sejam uma realidade. Há já muitos anos que a Siemens tem uma posição de liderança na área dos sistemas industriais digitais, por isso, desde cedo percebeu que a cibersegurança era uma parte integral e crucial da revolução digital. Diariamente, vemos o quanto isto é importante para os nossos clientes nos projetos que desenvolvemos em conjunto. Muitos já ambicionam ter sistemas e serviços digitais avançados nas suas operações, mas, sem a confiança que a cibersegurança proporciona, dificilmente estarão disponíveis para fazer as alterações e os investimentos necessários. O mesmo se aplica às infraestruturas críticas, às telecomunicações, à mobilidade ou à energia. A cibersegurança é essencial para todos estes setores.

Que estratégia segue a Siemens para a área da cibersegurança?
Enquanto empresa tecnológica, queremos ser um parceiro de confiança dos nossos clientes na área da cibersegurança, clientes que operam em setores tão críticos para o dia a dia das nossas sociedades e economias como os da indústria, da energia, da mobilidade ou das infraestruturas. Por isso, fazemos uma abordagem única à segurança cibernética, holística e baseada em dados, que inclui a segurança dos produtos, dos sistemas e das operações. Adaptamos as nossas metodologias de prevenção às necessidades de cada setor de atividade, e às potenciais ameaças a que estão sujeitos. E esta nossa abordagem abrange desde medidas mais genéricas até projetos de investigação avançada levados a cabo pelo Technology, o departamento central de Investigação & Desenvolvimento da Siemens AG, ou pelas várias unidades de negócio, países ou regiões onde a empresa está presente.

Este é hoje um dos pilares estratégicos da empresa? Porquê?
Sem dúvida, porque a cibersegurança é crucial para a transformação digital bem-sucedida dos negócios e dos diferentes setores de atividade. Para garantir a segurança dos dados e dos sistemas em rede, a cibersegurança deve ser integrada diretamente ao longo de toda a cadeia de valor. A Siemens foi uma das primeiras empresas a nível mundial a abordar esta temática de forma holística, protegendo a sua própria infraestrutura de tecnologias de informação e de operação, produtos, soluções e serviços, enquanto desenvolve e comercializa soluções inovadoras de cibersegurança. E, aproveito para mencionar, tem também uma grande tradição, competências e um vasto portefólio na área da proteção física das instalações (sistemas de deteção, alarme, evacuação e extinção de incêndio; e sistemas de segurança, como videovigilância, controlo de acessos, entre outros).

Luís Costa, especialista em Cibersegurança na Siemens Portugal

Conforme já mencionei, a empresa emprega atualmente 1.300 especialistas em cibersegurança em todo o mundo, incluindo hackers éticos que testam as vulnerabilidades dos sistemas e dos produtos. Tem também a operar, a nível global, cinco centros de cibersegurança, sendo um deles em Portugal, que monitorizam e protegem as suas próprias infraestruturas e as infraestruturas industriais de clientes específicos. A Siemens tem ainda responsáveis de cibersegurança nomeados em todas as unidades de negócio e países, aposta na formação contínua e sensibilização regular das suas pessoas para esta temática, e definiu a "Cibersegurança e Confiança" como uma das suas tecnologias core, o que faz com que esta seja uma das suas áreas foco em matérias de Investigação & Desenvolvimento. Estas tecnologias core são consideradas críticas para o sucesso dos clientes da empresa, com os quais trabalha em estreita colaboração e em ecossistemas abertos de inovação, com o intuito de alcançar os melhores resultados possíveis.

Que importância tem a participação da Siemens na aliança Charter of Trust, quer no que se refere ao negócio, quer no impacto do trabalho que estas organizações desenvolvem em conjunto com o objetivo de tornar o mundo digital mais seguro?
Uma base holística que gere confiança no mundo digital não pode ser alcançada por uma única empresa, Governo ou stakeholder. Tem de ser o resultado de uma colaboração próxima que envolva todas as partes interessadas. Com isso em mente, durante a Conferência de Segurança de Munique de 2018, a Siemens, juntamente com oito parceiros do setor industrial, apresentou a iniciativa global Charter of Trust (CoT) – um esforço coletivo proposto para empresas, sociedade, governos e todos os stakeholders interessados em construírem uma nova base para a confiança e a justiça num mundo cada vez mais digital. Em suma, esta iniciativa visa impulsionar avanços na cibersegurança em todas as indústrias e a nível mundial. Atualmente, a Charter of Trust conta com 18 membros e, desde a sua criação, lançou uma série de medidas para reforçar a cibersegurança, incluindo o princípio "Security by Default", que contempla as necessidades de cibersegurança logo desde a fase de conceção e disponibiliza produtos que integram medidas de segurança pré-configuradas. Além disso, os parceiros da CoT definiram requisitos base para os seus fornecedores, de modo a melhorar ainda mais a cibersegurança em todas as cadeias de fornecimento. A prioridade da CoT está agora na implementação de uma abordagem que inclua todas as indústrias, com o objetivo de avaliar a segurança das respetivas cadeias de fornecimento. Neste contexto, a comunidade crescente da Charter of Trust pretende disponibilizar informação, formação e outros recursos às empresas, principalmente às de pequena e média dimensão, e garantir a fiabilidade e a confiança da utilização da inteligência artificial nas soluções e ofertas digitais.
A iniciativa CoT colabora também regularmente com várias autoridades mundiais e instituições científicas para impulsionar os avanços na cibersegurança a nível internacional, e para harmonizar os esforços desenvolvidos nesta área para além das fronteiras nacionais e organizacionais. Neste âmbito, teve um importante papel na revisão das leis de segurança de TI na Alemanha e da Lei Europeia de Cibersegurança (European Cybersecurity Act), bem como em consultas governamentais levadas a cabo no Japão e na Austrália.

Quando foi criada esta equipa de cibersegurança e de que forma cresceu e evoluiu ao longo dos anos?
A equipa foi criada em 2014 como parte do hub de Tecnologias de Informação. Devido à qualidade do trabalho e à vontade constante de expansão do centro em Portugal, a equipa foi crescendo ao longo dos anos, tanto em número, como nos serviços prestados. Atualmente, com mais de 100 profissionais dedicados à cibersegurança, a Siemens em Portugal terá uma das maiores, senão a maior, equipa de cibersegurança do país. Para sustentar este crescimento numa área tão relevante e específica, a Siemens dedicou especial atenção à procura e formação de talento. Desde 2015 que temos, em permanência, vagas abertas para profissionais experientes e recém-graduados. Neste âmbito, desenvolvemos também programas de integração, requalificação e desenvolvimento de profissionais de outras áreas, programas de cibersegurança nacionais e colaboramos com diversas universidades, criando assim as condições para ter um cada vez maior número de profissionais formados nas múltiplas áreas tecnológicas da cibersegurança que operamos globalmente, a partir de Portugal e em colaboração com os outros hubs de cibersegurança no mundo Siemens.

Uma década depois da criação do Lisbon Tech Hub, que balanço faz?
É um balanço muito positivo. Quando este centro foi criado, em 2014, com 40 pessoas, previa-se que pudesse vir a ter 250 colaboradores. Hoje, 10 anos depois, já conta com mais de 1.400 especialistas que desenvolvem projetos para todo o mundo Siemens, em diversas áreas tecnológicas como a inteligência artificial, big data, desenvolvimento e teste de software, serviços na nuvem, cibersegurança e serviços de infraestrutura de tecnologias de informação. Trabalha também em estreita colaboração com as várias áreas de negócio da Siemens, como a indústria, as infraestruturas ou a mobilidade, para que estas possam propor as soluções mais inovadoras aos seus clientes.
E as perspetivas para o futuro são muito positivas, uma vez que o Lisbon Tech Hub poderá integrar até mais 200 pessoas altamente qualificadas até ao final do ano comercial (setembro de 2024), dando assim um importante contributo ao objetivo global da empresa de ter 4.000 colaboradores no Grupo até 2025, ano em que celebrará 120 anos de presença em Portugal.
A título de exemplo, e além da equipa de cibersegurança que integro, faz parte deste hub o Technology (T), o departamento central de Investigação & Desenvolvimento da Siemens AG que agora tem uma equipa em Portugal, e está em franco crescimento. Importa realçar que esta unidade, o T, só tem seis localizações a nível mundial, o que demonstra a relevância de Portugal no panorama de Investigação & Desenvolvimento mundial da Siemens AG. A equipa nacional conta com perto de 100 profissionais e trabalha em seis das 11 tecnologias core definidas pela Siemens AG (Circuitos Integrados & Eletrónica; Análise de Dados & Inteligência Artificial; Conectividade & Edge; Energia & Infraestruturas Sustentáveis; Produção Avançada & Circularidade; e Experiência do Utilizador). ■

OPINIÃO

PEDRO VIANA
DIRETOR DE PRÉ-VENDA, PORTUGAL E ESPANHA DA KASPERSKY

A INTELIGÊNCIA AO SERVIÇO DO COMBATE AO CIBERCRIME

Monitorizar, analisar, interpretar e mitigar as ameaças à segurança informática, que estão em constante evolução, representa um desafio significativo. Empresas de diversos setores enfrentam o desafio da falta de dados atualizados e pertinentes, essenciais para gerir os riscos associados à segurança das tecnologias da informação.

Os serviços de Inteligência de Ameaças da Kaspersky capacitam as organizações a anteciparem ameaças cibernéticas, fornecendo informações cruciais, deteção rápida e respostas eficientes a incidentes de segurança. A vasta experiência, o conhecimento profundo e a capacidade analítica da Kaspersky em cibersegurança reforçam a sua posição como parceiro confiável de proeminentes agências governamentais e entidades de aplicação da lei, incluindo a INTERPOL e os principais Centros de Resposta a Incidentes de Computador (CERTs).

FEEDS DE DADOS DE AMEAÇAS

Os ciberataques ocorrem diariamente, apresentando uma crescente frequência, complexidade e sofisticação, visando comprometer as defesas de empresas e entidades governamentais. Atualmente, os cibercriminosos empregam estratégias complexas e sofisticadas, incluindo sequências detalhadas de ataques, campanhas coordenadas e Táticas, Técnicas e Procedimentos (TTPs) personalizados, com o objetivo de desestabilizar os negócios ou de prejudicar os seus clientes. A Kaspersky Lab oferece Feeds de Dados de Ameaças, atualizados continuamente, para informar a sua empresa ou os seus clientes sobre os riscos e consequências associados às ciberameaças. Esses feeds são essenciais para ajudar a mitigar estas ameaças de maneira eficaz e para preparar a sua defesa contra ataques antes mesmo de serem lançados.

RECOLHA E TRATAMENTO

Os Feeds de Dados são compilados de fontes diversificadas e extremamente confiáveis, incluindo a Rede de Segurança Kaspersky, os nossos rastreadores web, o serviço de Monitorização de Botnet (ativo 24/7/365), armadilhas para spam, nossas equipas de investigação e parceiros estratégicos.

Depois, em tempo real, todos os dados agregados são cuidadosamente inspecionados e refinados usando múltiplas técnicas de pré-processamento, tais como critérios estatísticos, Sistemas Peritos Kaspersky Lab (sandboxes, motores heurísticos, scanners múltiplos, ferramentas de similaridade, perfis de comportamento, etc.), validação de analistas e verificação de listas brancas.

DADOS CONTEXTUAIS

Cada registo em cada Feed de Dados é enriquecido com contexto acionável (nomes de ameaças, carimbos de data/hora, geolocalização, endereços IPs resolvidos de recursos Web infetados, hashes, popularidade, etc.). Os dados contextuais ajudam a revelar o "quadro geral", validando e apoiando ainda mais a utilização alargada dos dados.

No contexto, os dados podem ser mais facilmente utilizados para responder às perguntas "quem", "o quê", "onde" e "quando", que conduzem à identificação dos seus adversários, ajudando-o a tomar decisões e acções atempadas específicas para a sua organização.

RASTREIO DE PHISHING

O phishing, e particularmente o spear-phishing direcionado, é uma das metodologias de fraude online mais perigosas e eficazes da atualidade. Os websites falsos capturam logins e palavras-passe para se apoderarem das identidades dos utilizadores e depois roubam dinheiro ou espalham spam e malware através de contas de email e plataformas de redes sociais comprometidas. Trata-se de uma arma poderosa no arsenal do cibercrime, e a frequência e diversidade dos ataques continua a aumentar.

E não são apenas as instituições financeiras que estão a ser atingidas. Todos, dos retalhistas online até aos ISP, passando pelas instituições governamentais, correm o risco de serem alvo de um ataque ativo de spear-phishing. Cópias perfeitas de um website, completas com toda a marca da empresa, ou mensagens que parecem vir diretamente dos seus executivos, podem facilmente convencer os utilizadores a entregar dados confidenciais, prejudicando-se a si próprios e causando enormes danos potenciais à empresa.

Um único ataque de phishing bem-sucedido pode ter um enorme impacto na empresa vítima. Além das perdas diretas, há todos os custos indiretos, como a limpeza de sites e contas comprometidos. E depois, claro, há os danos para a reputação, que podem ser os piores de todos - uma erosão da confiança dos utilizadores nos seus serviços online que pode fazer com que percam clientes e enfrentem desafios de credibilidade nos próximos anos.

Atualmente, o cibercrime não conhece fronteiras e as capacidades técnicas estão a melhorar rapidamente: estamos a assistir a ataques cada vez mais sofisticados, à medida que os cibercriminosos utilizam recursos da dark web para ameaçar os seus alvos.

EM CONCLUSÃO...

A inteligência de ameaças desempenha um papel crítico na capacidade das organizações de proteger os seus ativos digitais contra ameaças cibernéticas. Ao fornecer informações sobre ameaças emergentes, vulnerabilidades e táticas de ataque, capacita as organizações a tomar medidas proativas para fortalecer as suas defesas e responder de forma eficaz a incidentes de segurança cibernética. ■

ENQUADRAMENTO LEGISLATIVO CONTRIBUIRÁ PARA MAIOR CONSCIÊNCIA DOS RISCOS CIBERNÉTICOS

Aumento dos ciberataques e da sua sofisticação exige aceleração de esforços de gestão proactiva do risco. Diretiva europeia, que entrará em vigor até ao fim do ano, pretende uniformizar normas e garantir adoção de postura mais proativa das empresas face à segurança digital

Mariana Gomes, Senior Associate of FINEX na WTW Portugal

"Existe uma criminalidade organizada e um modelo de negócio altamente lucrativo que motiva a persistência deste fenómeno do cibercrime um pouco por todo o mundo", afirma Mariana Gomes. A Senior Associate of FINEX na WTW Portugal recorda o elevado número de ciberataques – cerca de 800 mil em 2023 –, a nível global que, apesar de tudo, representam uma estimativa, uma vez que muitas destas situações continuam a passar despercebidas ou não são identificadas como tal. A guerra na Ucrânia foi, na sua perspetiva, um catalisador, apesar de reconhecer que a maior parte dos ataques informáticos não decorrem de motivações políticas, mas sim de motivações financeiras.

Ainda assim, mesmo em países que não estão diretamente envolvidos neste conflito, têm-se verificado ataques a estruturas críticas e importantes da sociedade, como telecomunicações, energia, transportes entre outros.

Isto significa, acrescenta Mariana Gomes, que nenhuma organização, independentemente do setor que endereça ou da sua dimensão, está livre de perigo. Contudo, alerta para alguma desvalorização destas questões, a que acresce algum desconhecimento, em muitas empresas nacionais. É frequente, explica, as empresas "menorizarem a probabilidade de ocorrência de problemas (só ocorrem aos outros) e o impacto que podem ter (se acontecer algo basta ir comprar alguns computadores novos), e nada pode estar mais longe da verdade". Por um lado, reforça, todo o tipo de organizações está exposta a este tipo de situações quer diretamente (os seus próprios sistemas), quer indiretamente através da sua cadeia de fornecimento (os sistemas dos seus fornecedores), "o que tem sido abundantemente demonstrado por ataques mediáticos que afetam os mais diversos setores de atividade no nosso país".

Por outro lado, a responsável da WTW aponta igualmente a subvalorização da gravidade dos eventos, lembrando que os ataques informáticos podem ter consequências financeiras diretas, com perda de receitas (muitos modelos de negócio dependem da disponibilidade de sistemas e integridade de informação), custos avultados em consultoria (num evento catastrófico pode perder-se parte significativa da informação sob gestão e a reposição de capacidade operativa é difícil e demorada), gastos reputacionais (quebra de confiança dos clientes), ou responsabilidade de natureza contraordenacional para a organização. "É um tema que importa priorizar e que beneficiará do reforço legislativo que pretende acelerar os esforços de gestão proativa do risco", sublinha.

ANTECIPAR E MITIGAR OS RISCOS

Conhecer profundamente os efeitos que um ciberataque pode ter numa organização é o primeiro passo para a preparação. "Só percebendo os cenários e impactos poderemos desenhar medidas de mitigação e priorizar os investimentos", explica Mariana Gomes. Um caminho que a WTW ajuda as empresas a percorrer através de diferentes abordagens.

Em primeiro lugar, explica aquela responsável, "contribuímos para ajudar a quantificar o risco efetivo que determinada organização tem pois conseguimos estimar os impactos de incidentes". Esta informação é o ponto de partida para tomar decisões mais conscientes, priorizar planos de mitigação de risco, e definir planos de resposta a incidentes. Paralelamente, salienta, "poderemos ajudar o cliente a transferir parte do risco cibernético inerente para o mercado segurador, garantindo assim uma forma de alisar o impacto financeiro que estes eventos podem trazer para a organização".

Apesar do longo caminho a percorrer, a responsável da WTW acredita que a consciencialização das empresas começa a aumentar, nomeadamente, pelas exigências legislativas. Seis anos depois da entrada em vigor da diretiva europeia NIS – que tem como objetivo reforçar a resiliência do espaço europeu face à cibersegurança –, esta será substituída pela NIS2, que estará em vigor até ao final de 2024, e que reforçará o controle da segurança no ciberespaço dos estados-membros. "Acredito que a sensibilização do tecido empresarial português vai aumentar significativamente no próximo ano, ano e meio, mas quiçá não muito por mérito da pedagogia, mas por receio dos impactos contraordenacionais que a NIS2 vai implicar", conclui Mariana Gomes. ■

"É CRUCIAL QUE AS EMPRESAS ENTENDAM A NECESSIDADE URGENTE DE ANTECIPAREM E ESTAREM PREPARADAS"

A complexidade crescente das tecnologias da informação exige maiores níveis de automação, sem os quais não existe capacidade de resposta adequada aos desafios da cibersegurança. José Eduardo Fonseca, diretor na Kyndryl em Portugal, explica, em entrevista à *Exame Informática*, que precauções e que estratégias devem as organizações adotar para evitar ameaças que podem custar-lhes milhões de euros

Os ciberataques continuam a aumentar, especialmente desde o início da guerra da Ucrânia. Neste contexto, qual a estratégia da Kyndryl na área de Cibersecurity & Resilence?
Ao longo dos últimos anos, a percentagem de ataques cibernéticos aumentou substancialmente mesmo antes da guerra da Ucrânia. No período COVID, cerca de 60% das empresas em todo o mundo, implementaram em pouco tempo um crescente número de tecnologias para fazer face à remotização do trabalho, e fizeram-no com muitas, e naturais, preocupações operacionais, mas, em grande parte com um sistema de segurança muito limitado e pouco adequado. Adicionalmente, por via do trabalho remoto, cresceram exponencialmente os acessos às redes das organizações a partir de redes de casa, onde as preocupações com segurança são, na maioria das vezes, básicas. Isto originou um aumento de vulnerabilidades e um maior número das ameaças e ataques cibernéticos. Por outro lado, assistimos a uma proliferação de tecnologias de segurança que resolvem problemas muito restritos. Para enfrentar o desafio da segurança, as empresas tendem a investir em múltiplas ferramentas e, de seguida, enfrentam dificuldades para integrá-las e geri-las. Essa complexidade reduz a sua eficácia e mantém alguns dos riscos.

E a sofisticação das ameaças também é maior...
Com o nível de sofisticação, disrupção e destruição que os ataques hoje apresentam (como ransomware), efetuados por atores que percebem que o retorno financeiro pode ser significativo, é crucial que as empresas entendam a necessidade urgente de anteciparem e estarem preparadas para o caso de sofrerem um ataque e, com especial importância, conseguirem recuperar os seus serviços críticos. A Kyndryl é uma empresa focada em serviços de TI e infraestrutura, possui uma enorme experiência nestas áreas, bem como uma estratégia robusta de cibersegurança e resiliência para proteger as suas operações e as dos seus clientes, responder a ataques e recuperar dos mesmos. Para fazê-lo mantém um programa de gestão de segurança que inclui políticas, práticas, e controlos, além da formação contínua dos seus profissionais nesta área. O objetivo é minimizar o risco de perda de informações e de indisponibilidades por questões de segurança, criar 'awareness' e ter profissionais que tenham a conduta adequada nestas matérias, uma vez que têm acessos privilegiados aos sistemas no âmbito das suas funções.

A aposta na Kyndryl Bridge é uma das prioridades para este ano fiscal. Que impacto terá esta solução na gestão do negócio dos clientes, no que se refere à automação e utilização de plataformas inteligentes na gestão diária de incidentes e na sua prevenção?
As empresas enfrentam hoje uma necessidade urgente e sem precedentes para modernizar e transformar os seus processos de TI que são cada vez mais complexos. Os processos de negócios digitais e o poder de computação estão a tornar-se descentralizados, enquanto os volumes de dados crescem exponencialmente. A necessidade de "always on" a que esta nova era obriga, aliada ao negócio muitas vezes totalmente assente no digital, obriga a ter capacidade de resposta imediata, mas sobretudo capacidades de prevenção e antecipação das ocorrências. Esta complexidade crescente, decorrente das multitecnologias, multiclouds, aliada à exigência do 'always on', só se consegue com plataformas de integração que, com base em data analysis/insights e automação, permitem uma gestão feita pela tecnologia, acompanhada pelas capacidades técnicas e experiência dos nossos profissionais. Acreditamos que a gestão das TI tende para um patamar de complexidade que, sem recurso a estes níveis de automação, serão incomportáveis, quer em termos de profissionais necessários, quer em valores financeiros. A Kyndryl Bridge é uma plataforma diferenciada, que tira partido de modelos IA (Inteligência Artificial) que utilizam como base os nossos data-lakes, complementados com a experiência em gerir ambientes de TI complexos e "mission critical" que ajuda a gerir melhor, de forma mais eficiente e eficaz, e que permite evoluir a gestão de

— **José Eduardo Fonseca, diretor da Kyndryl em Portugal**

TI para os patamares que uma organização moderna necessita, com agilidade e capacidade de atuação para manter os sistemas funcionais para o negócio que suportam.

Que benefícios, e que poupanças traz esta solução para as organizações?
A Kyndryl Bridge permite que os clientes usufruam de operações de tecnologia mais estáveis e fiáveis com recurso a Intelligent Ops e automação para criar, e sobretudo gerir, ambientes mais fluidos e dinâmicos, que permitam às organizações capacitar-se de diversas tecnologias para se adaptarem às necessidades do mercado em mudança. As grandes vantagens são a rapidez de atuação preventiva (automatizada), o aumento da produtividade, melhores experiências dos profissionais e dos clientes, melhor controlo dos custos de gestão de TI, e, muito relevante, aumento da receita. Uma melhor capacidade de impulsionar objetivos importantes para o negócio, uma vez que ambientes que apresentam maiores níveis de disponibilidade, bem como uma organização que consegue um Go-to-market digital mais rápido, consegue melhorar os seus resultados de negócio. Uma plataforma que integra todas as ferramentas de gestão, permite saber a cada momento como estão a ser endereçados todos os eventos resultantes de incidentes, alarmes e outras atividades, utilizando automação para endereçar a grande maioria deles. A título de exemplo, a nossa operação em Portugal, trata mais de um milhão de eventos por mês de uma forma automatizada, e os que não são ainda tratados desta forma são analisados e evoluídos para que possam vir a ser automatizados no futuro. A própria Kyndryl Bridge indica-nos que casos de uso podemos e/ou devemos automatizar para aumentar estes níveis de automação. Tudo isto tem um enorme valor na rapidez de execução e no controlo dos custos das organizações.

A transformação dos sistemas de segurança comporta novos desafios para as empresas. Como garantir o equilíbrio entre os sistemas legacy e os novos?
A Transformação Digital tornou-se um imperativo para todas as organizações, tendo-se intensificado durante o período da pandemia com a utilização de sistemas de colaboração e com um enorme desenvolvimento do negócio através de canais digitais. Contudo, quando analisamos os surveys que interrogam os CIOs ou os CEOs, constatamos que em muitos casos, não se encontram totalmente satisfeitos com os investimentos realizados na sua transformação digital. Segundo a McKinsey, cerca de 70% dos líderes referem que a transformação está inacabada, em particular no que se refere à adoção de sistemas em cloud e, de acordo com dados da KPMG, 67% defende que a utilização de cloud ainda é limitada. Como consequência, a maioria das grandes empresas e instituições, deparam-se com arquiteturas de sistemas muito complexas onde os seus sistemas legacy baseados em arquiteturas tradicionais, muitas delas on site, têm de coexistir com novas aplicações modernas suportadas por clouds públicas, privadas ou híbridas. Paralelamente, os dados com volumes crescentes estão mais dispersos e, portanto, difíceis de utilizar e de gerir, aumentando a complexidade devido às normas de segurança. A velocidade de execução faz a diferença para conseguir ser dos melhores no mercado. E para consegui-lo é necessária uma infraestrutura de TI consistente, resiliente e inteligente. O novo modelo operacional e de gestão tem de conseguir tratar o legacy e o novo como apenas uma plataforma. Não nos enganemos, o legacy existe e existirá, pois as organizações não têm capacidade financeira, de recursos e/ou tempo para uma renovação total e, por isso, é tão importante a gestão eficiente e modernizada.

Que riscos enfrentam as organizações que não se munirem das ferramentas de segurança adequadas aos desafios do seu negócio e do mercado?
O risco é um fator crescente em todos os negócios e é cada vez mais uma questão acompanhada pela gestão de topo. A segurança torna-se um fator ainda mais relevante à medida que as empresas desenvolvem as suas estratégias de transformação de negócio para atender às exigências do digital e de um cenário económico remodelado num mundo pós-pandemia. É impensável que as organizações, em particular as que têm negócio suportado em tecnologia, não tenham uma estratégia de cibersegurança. Sem isso, é uma questão de tempo até terem o seu negócio destruído e irrecuperável, e desta forma desaparecerem.

Como podem as empresas prevenir-se e antecipar as ameaças?
Os líderes com visão de futuro sabem que a diferenciação é impulsionada pela transformação contínua. Incluir a segurança como parte base do desenho da transformação é vital, não pode ser visto como um adicional. É fundamental uma estratégia de cibersegurança em que se conjuguem ferramentas de proteção, deteção e verificação constante da adequação, bem como capacidade de recuperação. Tudo isto, além de ferramentas, inclui processos de recuperação e gestão de incidentes de segurança, políticas de segurança e formação. A cibersegurança é um problema de todos e a falha de uma parte pode comprometer o todo. ■

OPINIÃO

PEDRO FARINHA
MANAGING DIRECTOR
SHIFTLEFT

SOFTWARE SUPPLY CHAIN SECURITY, A PONTE ENTRE TECNOLOGIA E GESTÃO DE RISCOS

Nos últimos anos, a União Europeia tem respondido às crescentes preocupações com a Cibersegurança em todos os setores económicos através da produção de legislação e da promoção de iniciativas. Legislação como NIS, CRA e DORA representam marcos significativos nesse esforço, visando proteger infraestruturas críticas, dados sensíveis e setores económicos em geral contra-ataques cibernéticos, impondo requisitos mais rigorosos em termos de segurança dos sistemas de informação e gestão do risco operacional.

As imposições legais trazem o grande benefício, ainda que por imposição, de aumentar o conhecimento na organização e de adequar o grau de alerta dos seus órgãos de governo, sobre a importância do software que usam, desenvolvem e compram, fornecendo detalhes sobre como se protegerem, e protegerem os seus clientes e utilizadores.

A importância deste tema é reconhecida pela comunidade científica como ficou recentemente evidenciado no *International Workshop on Engineering and security of Critical Systems (EnCyCriS)*, inserido na *ICSE 24*, a *46ª Conferência Internacional sobre Engenharia de Software*, realizada em Lisboa na semana de 14 a 20 de abril, onde foi apresentada investigação sobre novas formas de certificação do *Software Bill of Materials (SBOM)* e tratamento de vulnerabilidades, ambos aspetos essenciais no *Software Supply Chain Security (SSCS)*.

Do ponto de vista do desenvolvimento de software, o conceito de SSCS não se restringe apenas ao software desenvolvido e à sua segurança intrínseca, mas à gestão de todos os riscos associados ao processo de desenvolvimento, incluindo os do produto final.

Frameworks como *SLSA* da *Open Source Security Fundation*, e *CIS* do *Center For Internet Security*, focam a proteção do *Supply Chain* no desenvolvimento de software que abrange quatro aspetos essenciais:

1. Código-Fonte
A garantia da integridade do código-fonte e da plataforma de gestão desse código é um dos pilares da segurança do software. Incluem-se aqui os aspetos da gestão dos utilizadores que acedem e podem alterar o código fonte; a imposição das regras de alteração desse código; proteção de dados confidenciais; proteção contra vulnerabilidades e prevenção de introdução de malware de forma intencional ou por desconhecimento;

2. Componentes de Terceiros
A composição de software é prevalente nesta indústria, mas é necessário conhecer quais e porque são necessárias essas dependências, bem como saber que riscos existem associados às mesmas. Como podemos atestar sobre a segurança desses componentes? Qual a fiabilidade do próprio SBOM desse componentes e do seu processo de desenvolvimento? Que exposição sobre licenciamento impõem?

3. Processo de Construção ("Build")
Pipelines e workflow são jargão comum associado aos temas *DevOps* e *CI/CD*, métodos comuns e prevalentes. Mas este processo de construção tem de ser ele próprio protegido e a sua integridade mantida. Como assegurar que o pipeline usado é o pretendido e que não foi adulterado propositadamente ou inadvertidamente?

4. Produto Final
O produto final pode ser um software final ou um componente de um produto final. É necessário assegurar a proteção desse produto único, e prevenir a sua alteração ou manipulação posterior. Também na distribuição, como assegurar que quem obtém o produto acede ao produto pretendido e não a uma cópia alterada? Em suma, o SCSS permite provar que o software que se disponibiliza foi aquele que foi criado, certificado e atestado.

Supply Chain Security, é um tema vasto, mas de elevada criticidade no contexto económico, social e tecnológico atual e que afeta todas as organizações, independentemente do setor em que atuam.

Quer seja uma empresa que "apenas" usa software, produzido por terceiros, e que licencia, ou uma empresa que desenvolve e mantém – diretamente ou por terceiros – software, é essencial saber a proveniência do software e conseguir atestar "do que é feito" e "como é feito". Não apenas porque está obrigada por legislação mais ou menos sectorial, mas porque é forma eficaz para conseguir proteger o negócio, clientes e parceiros e a sociedade. ■

MESTRADO EM SEGURANÇA INFORMÁTICA GARANTE EMPREGABILIDADE DENTRO E FORA DE PORTUGAL

O curso, ministrado na Universidade de Coimbra, reforça competências técnicas em diferentes vertentes relacionadas com esta temática, tais como criptografia, privacidade, comunicações e infraestruturas seguras, segurança de software e aspetos legais de privacidade e cibersegurança

Especialização temática ajustada às necessidades atuais do mercado, de que é exemplo o alinhamento com as competências definidas pela ENISA ECSF (European Cyber-Security Skills Framework) para cargos relacionados com cibersegurança, e fortes parcerias com academias internacionais, empresas nacionais e multinacionais e com o Centro Nacional de Cibersegurança (CNCS) são alguns dos fatores diferenciadores do Mestrado em Segurança Informática (MSI - **www.dei.uc.pt/msi/**), da Universidade de Coimbra.

O curso, lançado no ano letivo de 2017/2018 "com o objetivo de dar resposta à procura de profissionais na área de Cibersegurança e às necessidades criadas pelas diretivas europeias e pelos desafios societais relacionados com a segurança e privacidade de empresas e cidadãos como, por exemplo, do Regulamento Geral de Proteção de Dados (RGPD)", como explica Paulo Rupino Cunha, coordenador do MSI, conta anualmente com 20 vagas, e destina-se quer a alunos que ainda estão a completar o seu ciclo de estudos, quer àqueles que já estão inseridos no mercado de trabalho.

É por esta razão que a flexibilidade é outra das grandes mais-valias do Mestrado em Segurança Informática, que funciona em regime pós-laboral. "Grande parte das aulas têm início a partir das 18h, as aulas teóricas são difundidas por streaming (para permitir a participação remota) e gravadas, e parte substancial dos trabalhos práticos pode ser feita de forma assíncrona, com apoio remoto dos docentes", destaca Bruno Miguel Sousa, vice-coordenador do MSI.

Adicionalmente, e devido à crescente procura por estudantes internacionais, nomeadamente de países como o Brasil, a República Checa ou a Ucrânia, todos os conteúdos são lecionados em inglês. Uma opção que, na opinião de Paulo Rupino Cunha, é essencial, "uma vez que as principais saídas profissionais do MSI são multinacionais e empresas de média e grande dimensão no espaço nacional e europeu, nos setores de TIC, telecomunicações, consultoria, banca e serviços".

COMPETÊNCIAS COM FORTE VERTENTE PRÁTICA

Criptografia, privacidade, comunicações e infraestruturas seguras, segurança de software e aspetos legais de privacidade e cibersegurança são algumas das competências técnicas especializadas a que os alunos do MSI têm acesso. Muitas destas competências teóricas são reforçadas com uma forte componente prática, nomeadamente, através de aulas ministradas por professores com extensa experiência e por representantes de empresas convidadas - Deloitte, IBM, Banco CTT, Ethiack, Critical Software, são apenas alguns exemplos -, o que permite "um contacto privilegiado entre as empresas e os alunos no departamento de engenharia informática, onde o curso decorre", salienta Bruno Sousa.

Da interação com o mercado empresarial nascem igualmente ideias e temas para teses de mestrado, que beneficiam também do contacto e da colaboração com academias internacionais, como a Automotive CyberSecurity Academy (ACSA), ou com o CNCS. "A colaboração com o CNCS centra-se sobretudo no programa C-Academy, no qual docentes do curso MSI participam com a elaboração de materiais formativos e em módulos de formação", explica Paulo Rupino Cunha.

Já a colaboração com a ACSA, sublinha Bruno Sousa, "teve o seu ponto alto, em 2023, com a organização de uma escola de Verão na Universidade de Coimbra, que contou com a participação de cerca de 30 alunos internacionais, na temática de cibersegurança para automóveis". A edição de 2024 decorrerá na Universidade de Salerno, em Itália. ■

OPINIÃO

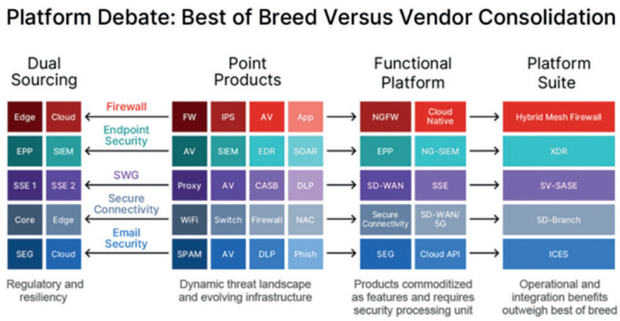
JOHN MADDISON
CHIEF MARKETING OFFICER
AT FORTINET

BEM-VINDOS À ERA DAS PLATAFORMAS

O debate sobre plataformas está na moda. Contudo, este não é um tema novo. Sempre existiu uma discussão transversal a todos os setores sobre os melhores produtos versus plataformas integradas. Ao implementar uma plataforma de cibersegurança na sua organização, é crucial pensar em "plataforma" como uma jornada.

A INDÚSTRIA DA CIBERSEGURANÇA ESTÁ PRONTA PARA ENTRAR NA ERA DAS PLATAFORMAS?

O grande debate sobre plataformas deveria começar com outra pergunta: Porque é que ainda existem produtos pontuais? A resposta reside na natureza dinâmica da cibersegurança e da infraestrutura. Devido à constante mudança dos vários tipos de ameaças, a indústria vai necessitar sempre de criar defesas, o que significa o desenvolvimento de novos produtos pontuais. E como a infraestrutura continua a evoluir para responder às necessidades de operações dinâmicas, vão ser criados, necessariamente, novos produtos pontuais para fazer face a novos riscos e oportunidades.



Contudo, à medida que certos produtos pontuais se tornam estáveis ou comoditizados ao longo do tempo, podem tornar-se componentes de uma plataforma funcional. Faz todo o sentido combinar numa única plataforma múltiplos componentes usados comumente para simplificar operações e integrar funções críticas. Mas, para o fazer corretamente, é necessário existir uma interoperabilidade profunda entre esses elementos. Isto resulta noutro cenário muito pior e que os clientes começam a aperceber-se: Na corrida para lançar uma plataforma no mercado, as grandes empresas adquirem produtos pontuais de outros fornecedores. Em vez de dedicarem tempo para integrar totalmente as funções e operações numa solução unificada, limitam-se a colocar a sua marca e a acrescentar um rótulo de "plataforma" ao pacote resultante.

Algumas empresas de maior dimensão, especialmente as que têm requisitos regulamentares, estão agora a adotar uma abordagem adicional ao conjunto de plataformas: plataformas funcionais de fonte dupla e até produtos pontuais. Esta situação é motivada pela necessidade de reduzir as despesas gerais e de gestão através da conversão de plataformas, atenuando simultaneamente os riscos através da adoção de uma abordagem de plataforma por camadas.

EMBARQUE NA SUA JORNADA

Todas as empresas gostariam de reduzir custos operacionais enquanto aumentam a eficácia da sua postura de segurança. Uma abordagem de plataforma de cibersegurança pode alcançar esse objetivo ao integrar produtos pontuais, reduzindo as despesas gerais e permitindo a automatização nativa em vários produtos. Algumas empresas optarão por implementar exclusivamente plataformas funcionais, enquanto outras vão avançar para os conjuntos de plataformas ou irão escolher a fonte dupla. O objetivo é embarcar na jornada mais adequada às suas necessidades e deixar de utilizar exclusivamente produtos pontuais.

No entanto, nem todas as plataformas são criadas da mesma forma e nem todos os fornecedores que reivindicam a "plataforma" podem apoiá-lo. Muitas soluções de fornecedores, que agora estão a ser rotuladas como plataformas, são na realidade compostas por produtos muito distintos com diferentes sistemas operativos, linguagens de programação, estruturas de dados, APIs e consolas de gestão. Em vez de fornecerem um sistema verdadeiramente integrado, são simplesmente soluções díspares agrupadas numa plataforma superficial.

A Fortinet foi fundada há mais de duas décadas com base no princípio da convergência de redes e de segurança. Atualmente, a plataforma Security Fabric é composta pelo portfólio de produtos mais integrado e mais aberto do setor, apoiado por um sistema operativo (FortiOS), um agente unificado (FortiClient), uma consola de gestão (FortiManager), um data lake (FortiAnalyzer), APIs abertas e integração com mais de 500 produtos de terceiros, incluindo os dos nossos concorrentes.

A melhor parte é que pode fazer tudo na plataforma Security Fabric da Fortinet ou usar os seus elementos como uma base sólida para começar a incorporar plataformas funcionais ou conjuntos de plataformas na sua infraestrutura existente.

Quando falar com fornecedores sobre uma solução de plataforma, é vital olhar para a estrutura da mesma. Existe realmente um sistema operativo único, uma consola de gestão, um motor de análise único, um data lake e APIs uniformes que sustentam a plataforma que está a considerar? Ou estará simplesmente a transferir a complexidade da sua abordagem do produto pontual existente para um formato diferente? Esta escolha poderá ter um impacto significativo na segurança e operações gerais. ■

O Chef na recepção?

Faça o que sabe fazer melhor. Da segurança dos dados dos seus clientes trata a Vodafone Business.

Somos muito mais do que comunicações.
Somos soluções Smart de Cibersegurança que garantem a proteção de dados e equipamentos.

vodafone.pt/business

Together we can
vodafone
business