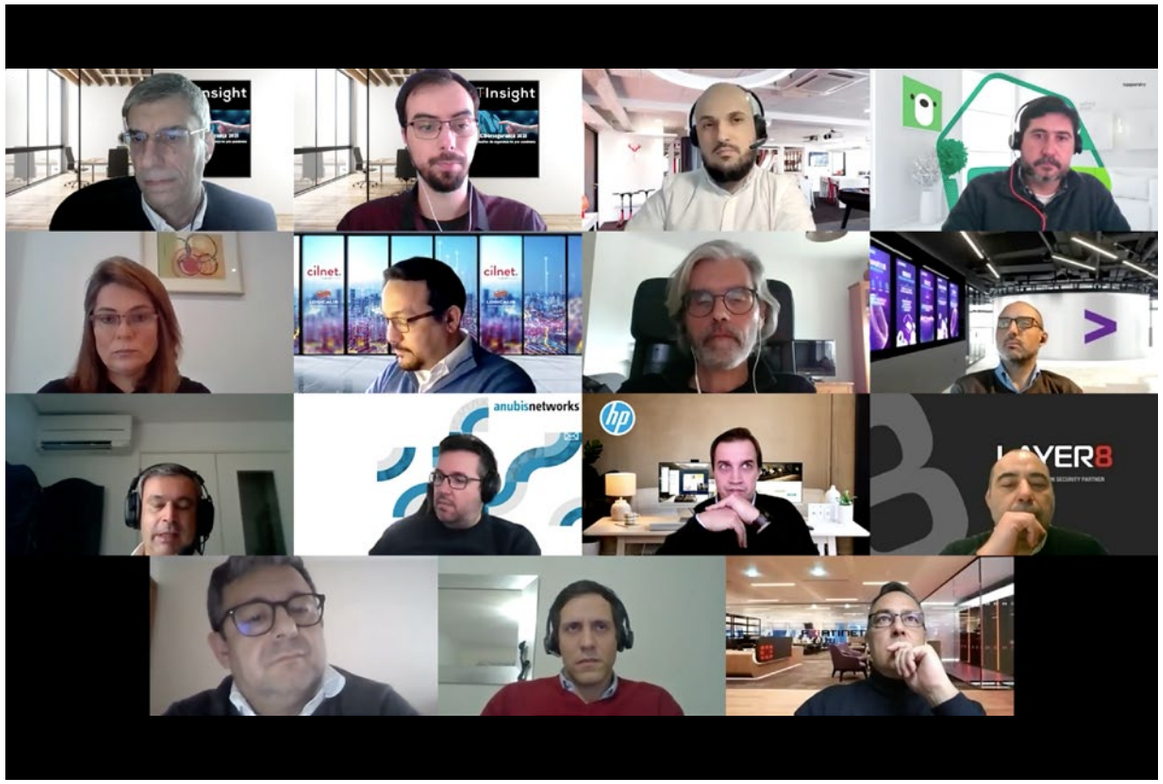
A CIBERSEGURANÇA DAS ORGANIZAÇÕES É MAIS IMPORTANTE DO QUE NUNCA

Com a transformação digital a acelerar, as organizações devem apostar na cibersegurança, mas, por vezes, acabam por ficar num segundo plano de investimento. Anubis Networks, Accenture, Cilnet, Claranet, Fortinet, HP Inc., IBM, Kaspersky, Layer 8, Nexllence, Noesis, S21sec e Warpcom dão a sua opinião sobre o mercado nacional de cibersegurança.

RUI DAMIÃO

PARA VER O VÍDEO CLIQUE SOBRE A IMAGEM



- A IT Insight realizou a sua habitual mesa redonda de forma digital, através de uma plataforma de videoconferência -

A CIBERSEGURANÇA sempre foi importante, mas, depois de os colaboradores começarem a trabalhar a partir de casa, passou a ter outra relevância para as organizações. Num cenário pós-pandémico é, agora, claro que o *workplace* será, sempre que possível, híbrido e móvel.

A responsabilidade de manter as redes seguras, garantir que os sistemas permanecem resilientes contra violações e tomar várias medidas para proteger os dados e a sua integridade de ameaças cibernéticas, é cada vez mais importante, uma vez que os cibercriminosos estão mais ousados nas suas tentativas de invadir os sistemas. Além do mais, a recente pandemia abriu possíveis pontos de brecha que, antes, poderiam não existir na organização.

INVESTIMENTO DURANTE A PANDEMIA

Com os colaboradores a trabalhar a partir de casa, o perímetro de ataque aumentou. Nem todas as organizações estavam preparadas para a realidade e, numa primeira fase, a escolha de investimento não passou necessariamente pela segurança.

O PERÍODO PANDÉMICO OBRIGOU A REPENSAR OS PLANOS DE EMERGÊNCIA E CIBERSEGURANÇA DAS ORGANIZAÇÕES

Pedro Coelho, Computing Area Category Manager da HP Inc., refere que, "para quem olha do ponto de vista dos postos de trabalho pessoais, o que se notou é que o período pandémico obrigou a pensar um pouco melhor quais eram as medidas de proteção. Depois do primeiro impacto em que muitas vezes se ativaram planos de emergência, sentimos – ao longo da segunda metade de 2020 – uma maior preocupação com as questões de segurança e voltou a subir na lista de prioridades dos principais responsáveis de informática".

José Borges Ferreira, CEO da Anubis Networks, indica que "viemos de um mundo muito tradicional onde estávamos habituados a ter a segurança dentro do perímetro. Quando se foi para casa, tudo isso se desmanchou; não havia uma preparação de acessos remotos, de controlo de informação e gestão de acessos. Isso foi a grande diferença do trabalho remoto, não tanto de tecnologia, mas sim de procedimentos. As empresas não estavam organizadas para trabalhar remotamente do ponto de vista de gestão de informação e segurança".

Nuno Baptista, Associate Director e Responsável pela área de Security da Accenture, explica que "há uma necessidade de investir em pessoas especializadas. A complexidade do problema faz com que as organizações tenham muita dificuldade em endereçar todos estes temas. A forma como as empresas encararam o tema difere com a sua maturidade; é um bocado difícil generalizar a forma como as empresas foram impactadas pela pandemia, mas a complexidade é muito grande e nem todas as organizações têm capacidade para o fazer".

INVESTIMENTO ESTRATÉGICO

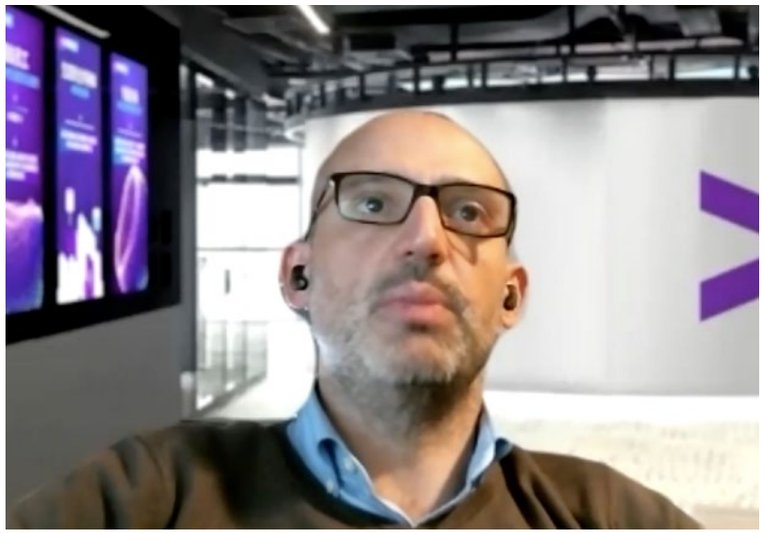
David Santos, BDM de Cybersecurity da Cilnet, afirma que "não existe uma empresa tipo que se consi-

- José Borges Ferreira -
CEO, Anubis Networks

"Os algoritmos vão permitir tomar decisões para algo que não conhecemos"

- Nuno Baptista -
Associate Director, Responsável pela área de Security, Accenture

"Os ataques de engenharia social vão continuar a evoluir e a aproveitar todas as fragilidades"



- Nuno Baptista, Accenture -

- José Borges Ferreira, Anubis Networks -

- David Santos, Cilnet -

ga caracterizar; cada uma tem a sua especificidade. O que temos vindo a verificar é que se começa a ter alguma noção que é preciso apostar na cibersegurança, mas muitos deles sentem-se perdidos porque não sabem por onde começar. Não podemos continuar a manter o diretor de IT a fazer também segurança porque o nível de *skills* são completamente diferentes. Este tipo de transformação é bastante complexo".

David Grave, Senior Cybersecurity Consultant da Claranet, diz que "muitas empresas não tinham os seus processos preparados e tiveram de recorrer em muitos casos aos VPN porque ainda tinham os processos dentro de casa; estas foram as empresas que tiveram mais dificuldade em se adaptar". No entanto, é preciso admitir que "o teletrabalho veio para ficar"; para isso, as empresas não podem viver sem a cloud e sem soluções escaláveis se querem manter o teletrabalho a funcionar de forma segura nas organizações.

Paulo Pinto, Business Develop Manager da Fortinet, menciona que, "se inicialmente as empresas se apressaram a confinar e a arranjar soluções mais pontuais para permitir o trabalho remoto, desde o início deste ano que se nota uma abordagem mais estratégica que se foca no médio e no longo prazo. As empresas procuram ser mais abrangentes e incluir todos os elementos do edge, que estão pendurados na cloud

- David Santos -
BDM de Cybersecurity, Cilnet

"Não podemos continuar a manter o diretor de IT a fazer também segurança porque o nível de skills é completamente diferentes"

- David Grave -
Senior Cybersecurity Consultant, Claranet

"É preciso pensar como é que se asseguram as ligações à cloud que já estão fora da infraestrutura"

O NÚMERO DE VIOLAÇÕES DE DADOS E REGISTOS COMPROMETIDOS ATINGIU O NÍVEL MAIS ALTO EM 2020

e nos pontos remotos, e com o requisito de controlo e visibilidade sobre os dispositivos".

TRABALHO REMOTO

Apesar do crescimento contínuo do investimento em cibersegurança ao longo dos últimos anos, o número de violações de dados e registos comprometidos, assim como ataques de ransomware, atingiu o nível mais alto no ano passado. No entanto, é preciso perceber se este crescimento se deveu ao trabalho remoto apenas, ou se às deficiências na segurança das infraestruturas que já existiam no período pré-pandémico.

António Bacalhau, Senior Security Sales Specialist da IBM, explica que "para além da grande maioria das empresas estar muito focada no tradicional, dentro do perímetro de trabalho, assim que começou o trabalho remoto o perímetro mudou e deixou de ser tão controlado. As organizações deixaram de ter tanta visibilidade dos seus ativos digitais e, assim que isso aconteceu, perderam a capacidade de os monitorizar e, à partida, ficaram mais vulneráveis e aumentaram o risco de ataque".

Élio Oliveira, Territory Channel Manager & SMB da Kaspersky, afirma que existiram "muitas decisões *ad hoc*. Muitas decisões tiveram de ser tomadas com as informações que tinham de uma forma muito rápida e espontânea. Quando falamos em colocar o PC debaixo do braço, levar para casa e começar a trabalhar, só foi necessário porque as empresas tiveram de garantir a continuidade do negócio. Também é preciso olhar para o nosso tecido empresarial e perceber quem é que tem um plano de continuidade de negócio e que empresas não têm".

MUITAS VEZES, NÃO HOUVE TEMPO PARA ADAPTAR OU IMPLEMENTAR PROCESSOS E FERRAMENTAS DE CIBERSEGURANÇA

Fernando Cardoso, COO da Layer 8, refere que, "de facto, existiu um aumento de ciberataques feito por cibercriminosos que são oportunistas; aproveitam um momento de maior fragilidade e incerteza para nos atacarem. Acho que ninguém tem dúvidas que a maioria dos ataques não são direcionados a sistemas, mas às pessoas; quando as pessoas estão mais frágeis e a viver momentos de maior incerteza, é aí que os atacantes conseguem ter mais êxito. Houve um aproveitamento do que está a acontecer para criar várias campanhas de cibercrime".

FRAGILIDADES ANTIGAS

Alexandre Costa, Head of Industry Executive da Nexllence, indica que, "em casa, o nível de segurança é muito mais baixo do que numa empresa. Notámos foi um aumento exponencial de vendas de licenciamento de VPN o que mostra que a maior parte das empresas em Portugal não estavam preparadas para esta mudança repentina. Há vários tipos de empresas que têm infraestruturas críticas para o Estado tem um nível de maturidade de segurança superior que a maioria do tecido empresarial português não tem".

Nuno Cândido, Infrastructure Solutions Senior Manager da Noesis, diz que "um grande número de ataques do ano passado não se deu apenas por causa da pandemia ou ao facto das pessoas trabalharem remotamente, mas a um conjunto mais diverso de fatores. Em termos de segurança, não houve tempo para adaptar ou implementar processos e ferramentas que permitissem suportar esta mudança tão repentina; tem de existir prioridades e isso levou a que as empresas ficassem mais desprotegidas, causando mais ataques".

Carla Zibreira, Head of Consulting da S21sec, menciona que "não houve uma alteração do contexto de risco; o que houve foi uma alteração brutal do ecossistema de riscos das organizações perante o cenário da pandemia. A pandemia trouxe alterações muito específicas – nomeadamente nos processos de negócio e à forma como são desempenhados e implementados. Isto veio alterar o equilíbrio dos vários riscos e da probabilidade que os riscos tinham de acontecer. Também existiu pouca preparação das organizações para responder a estes riscos".

- Paulo Pinto -
Business Develop Manager, Fortinet

"A automação e o machine learning vão ter um papel primordial no apoio às equipas de cibersegurança"

- Pedro Coelho -
Computing Area Category Manager, HP Inc,

"Quem está a pensar em como se vai proteger deve considerar em se proteger para o que existe e para o que não existe"

O TEMA DA PANDEMIA FOI UM DOS TEMAS MAIS UTILIZADOS PARA REALIZAR CIBERATAQUES CONTRA OS COLABORADORES DAS ORGANIZAÇÕES

EVOLUÇÃO DAS CIBERAMEAÇAS

Ao longo dos anos, as ameaças foram evoluindo. As empresas e os utilizadores já não têm de se preocupar com o 'simples' vírus informático, mas sim com uma miríade de ciberameaças cada vez mais complexas.

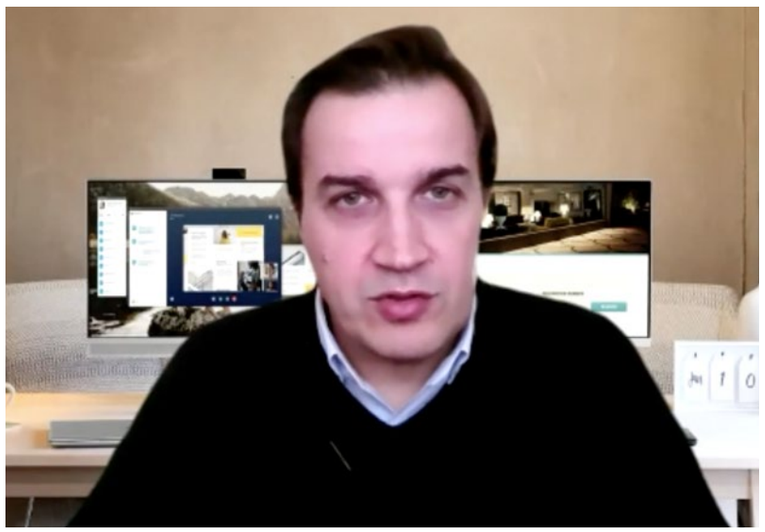
Nuno Baptista, da Accenture, explica que "os ataques de engenharia social, o phishing, vão continuar a evoluir e a aproveitar todas as fragilidades acrescidas que as pessoas têm sentido. Por outro lado, vemos que as táticas, as técnicas e os procedimentos dos atacantes estão a evoluir, ameaçando muito a continuidade do negócio. Vemos ataques direcionados e muito sofisticados que colocam em risco os dados da organização; antigamente, via-se a encriptação dos dados, mas agora vemos a exfiltração dos dados".

Bruno Gonçalves, Business Unit Manager – Cybersecurity & Public Safety da Warpcom, afirma que "todos os dias nos deparamos com ataques mais sofisticados e avançados e com um impacto brutal para as organizações. Atualmente, a indústria responde tendo em conta a sua maturidade. Dependendo dos setores e das organizações, há quem tenha uma maturidade grande e uma perceção do risco, analisando e percebendo as ameaças que existem para criar controlos efetivos para dar resposta, mas uma grande parte das organizações ainda não tem esta maturidade".

Focando-se nos emails, José Borges Ferreira refere que, "às vezes, o aumento da sofisticação é contraprodutivo; as coisas simples funcionam. A evolução passa por mecanismos de machine learning que permitam ler e analisar o conteúdo do email para perceber se o que está nos anexos são ameaças ou não. É preciso subir o jogo onde estes processos automáticos permitem, também, criar algumas

- David Grave, Claranet -

- Paulo Pinto, Fortinet -



- Pedro Coelho, HP Inc -

- António Bacalhau, IBM -

defesas" contra as ameaças que chegam às organizações diariamente.

FOCO NO UTILIZADOR

David Grave, da Claranet, indica que "nem todas as clouds são iguais; podemos estar num cloud provider de excelências e as configurações não serem as melhores. Gerir uma infraestrutura *on-premises* é muito diferente de gerir uma infraestrutura na cloud. A cloud não é simplesmente pegar nos nossos servidores, virtualizá-los e fazer a transposição para a cloud. É preciso pensar como é que se asseguram as ligações à cloud que já estão fora da minha infraestrutura; não posso apenas colocar uma firewall à frente dos servidores".

Paulo Pinto diz que "com a capilaridade das redes, com os *smart devices* que se usam e com os sistemas que já temos em casa, há uma maior porta de entrada. O que se coloca em casa é vantajoso, mas é uma porta de

MINIMIZAR OS RISCOS DE UM CIBERATAQUE É UMA PRIORIDADE PARA A MAIORIA DAS ORGANIZAÇÕES MUNDIAIS

entrada muito grande para se conseguir um conjunto de informações sobre o sujeito para depois ou tentar entrar dentro destes dispositivos, ou saltar para os dispositivos corporativos. Isso é uma das portas mais capilares para entrar atualmente e que é difícil de contornar porque não é uma questão tecnológica".

David Santos, da Cilnet, menciona que "as coisas estão cada vez mais específicas. O diferente tipo de ataque existente ou é o direcionado para a empresa, ou é através de phishing. No entanto, é preciso não esquecer que a entrada de qualquer ataque ou é de dentro para fora ou de fora para dentro e as medidas que temos de tomar têm de ser completamente diferentes. A primeira capacidade onde todas as empresas devem atuar é a formação ao utilizador; é preciso dotar todos os colaboradores de todos os tipos de ataques existentes".

Pedro Coelho aponta que "nestas questões da segurança, são sempre bem-vindos conceitos como sobreposição de várias camadas de proteção; a redundância acaba por ser bem-vinda nesta ótica da segurança. Outro conceito que faz sentido é planear para o pior cenário; se estivermos a planear para o pior cenário, estamos muito mais bem preparados para todos os outros. Quando se fala em evolução das ciberameaças, quem está a pensar em como se vai proteger deve considerar em se proteger para o que existe e para o que não existe".

MINIMIZAR OS RISCOS

Um estudo realizado por uma empresa do setor de cibersegurança indica que 51% das empresas consideram que minimizar os riscos de ciberataque são uma prioridade para as organizações mundiais.

- António Bacalhau -
Senior Security Sales Specialist, IBM

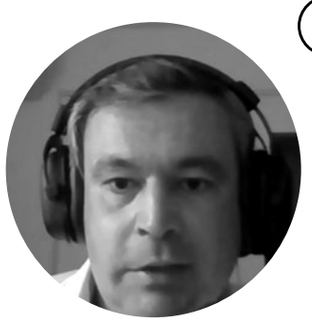
"As empresas estão mais conscientes dos impactos financeiros e reputacionais que os ataques podem ter"

- Élio Oliveira -
Territory Channel Manager & SMB, Kaspersky

"Muitas decisões tiveram de ser tomadas com as informações que tinham de uma forma muito rápida e espontânea"

- Fernando Cardoso -
COO, Layer 8

"A maioria dos ataques não são direcionados a sistemas, mas às pessoas"



- Alexandre Costa -
Head of Industry Executive, Nexllence

"DevSecOps é vetor de investimento muito forte nas empresas que têm uma maturidade maior em cibersegurança"

É EXPECTÁVEL QUE O RANSOMWARE CONTINUE A SER UMA AMEAÇA PARA AS ORGANIZAÇÕES

Fernando Cardoso afirma que "tudo tem a ver com a maturidade que as empresas têm e, de certo modo, a apetência ao risco. Quando fazemos bem o nosso trabalho em cibersegurança, os nossos sucessos são invisíveis; quando falhamos, o nosso trabalho é altamente visível. Ou há esta maturidade para a cibersegurança, ou as empresas só acordam para a prioridade de minimização de riscos quando algo acontece e as ciberameaças estão a evoluir a um bom ritmo, também com a massificação da utilização de dispositivos".

António Bacalhau sente que "há uma estabilização dentro do 'novo normal'. As empresas estão mais conscientes dos impactos financeiros e reputacionais que os ataques podem vir a ter dentro das suas organizações. Temos vindo a assistir a uma transformação digital quase global na maioria das empresas. No entanto, é preciso mostrar às empresas como se deve investir em cibersegurança; acho que a aproximação correta é que conseguimos fazer uma gestão completa, mas é preciso explicar como devem investir o seu *budget* em cibersegurança".

Pedro Coelho (HP) indica que, "em termos de investimento nesta área, é preciso ter uma abordagem estruturada que terá de começar pelos *endpoints*. Os próprios dispositivos IoT podem ser veículos de propagação de ameaças" e também devem ser protegidos. "Temos de nos preparar para um cenário em que o ransomware continuará a ser uma realidade muito pertinente, não só na ótica de exfiltração de dados, como também aliado aos desafios que o RGPD coloca, com o perigo desses dados se tornarem públicos".

INVESTIMENTO ESTRUTURADO

Alexandre Costa refere que, "este ano, tem existido um forte investimento em *Security-as-a-Code*, no-

meadamente na parte de DevOps. Os clientes procuram automatizar o processo de DevSecOps, que é uma área que traz grandes vantagens não só na parte de perímetro, mas também na parte de desenvolvimento de software e a segurança de software e API. Este é um vetor de investimento muito forte nas empresas que têm uma maturidade maior na área de cibersegurança".

Nuno Cândido, da Noesis, revela que "o mercado nacional ainda está atrás do mercado internacional. No entanto, temos assistido a um aumento significativo da prioridade do investimento em cibersegurança. Também vejo que temos um país que navega a várias velocidades, ou seja, as grandes empresas têm consciência e investimento de forma estruturada, e depois temos o mercado mais baixo em que a situação é muito diferente e onde é preciso um amadurecimento para que seja possível implementar processos eficazes".

Élio Oliveira nota que "há uma intenção das empresas para minimizar o impacto dos riscos e procuram proteger-se contra ameaças externas. Mas, até à data, as coisas têm sido feitas um pouco *ad hoc*. As empresas começam a olhar para a cibersegurança com uma estratégia já identificada. Enquanto fabricantes, temos o papel de evangelizar os clientes e explicar as necessidades que existem e porque se deve ir por um determinado caminho, porque é que é importante, por exemplo, a resposta automática a incidentes, entre outros".

- Élio Oliveira, Kaspersky -

- Fernando Cardoso, Layer 8 -

- Alexandre Costa, Nexllence -

AINDA QUE A INTELIGÊNCIA ARTIFICIAL NÃO SEJA ALGO NOVO, SÓ AGORA É QUE ESTÁ A SER UTILIZADA REGULARMENTE EM CIBERSEGURANÇA

INTELIGÊNCIA ARTIFICIAL

A Inteligência Artificial (IA) é cada vez mais utilizada em todo o IT. Na cibersegurança, terá um papel fundamental tanto para quem defende, como para quem ataca.

Carla Zibreira explica que "começamos a olhar para a inteligência artificial como uma solução que nos vai ajudar na capacidade de inteligência e na interpretação dessa inteligência ao nível da segurança, para além de ajudar na análise de informação massiva, por exemplo, de malware. Este tipo de ferramentas têm sido implementadas nesse sentido, no apoio e na ajuda" que podem dar às equipas de cibersegurança das organizações. Por outro lado, ainda se está a perceber o real alcance que estas ferramentas podem ter na proteção das empresas.

Bruno Gonçalves diz que "esta nova realidade de machine learning e inteligência artificial já começa a ser utilizada como ferramenta para ataques e defesa. Traz uma nova realidade para nós, será um novo desafio. Antes de chegarmos à parte de conseguir responder, temos de ganhar visibilidade e isso é um caminho que tem de ser feito. Vamos precisar de ganhar rapidamente maior visibilidade daquilo que está a acontecer dentro da infraestrutura das organizações e são precisas tecnologias que permitam suportar esta resposta".

António Bacalhau (IBM) indica que "a inteligência artificial já não é uma coisa nova. Há 20 anos, já programávamos sobre isso; não havia era capacidade. A cloud e o preço do *data storage* a baixar aumentou bastante esta capacidade. O que acontece é que à medida que os ataques cibernéticos têm vindo a aumentar, tem aumentado o volume e a complexidade dos mesmos. A inteligência artificial vai ajudar as operações de segurança – principalmente as que têm menos recursos – a ficarem à frente dessas ameaças".

APOIO ÀS EQUIPAS

Nuno Baptista (Accenture) afirma que "a inteligência artificial e o machine learning são um suporte daquilo que fazemos atualmente – e vamos continuar a fazer – não só na cibersegurança, mas também de uma forma mais transversal. Ao nível das pessoas e dos processos, tudo o que é análise comportamental

- Nuno Cândido -
Infrastructure Solutions Senior Manager, Noesis

"Temos assistido a um aumento significativo da prioridade do investimento em cibersegurança"

- Carla Zibreira -
Head of Consulting, S21sec

"Houve uma alteração brutal do ecossistema de riscos das organizações perante o cenário da pandemia"

relativamente à forma como utilizamos os dispositivos e os dados, gera tanta informação que a única forma de a trabalhar é com tecnologias de machine learning e inteligência artificial que nos permitem prever comportamentos potencialmente perigosos e atuar em conformidade".

David Santos (Cilnet) refere que "é cada vez mais utilizado pelos atacantes a orquestração e o machine learning. Prevejo que, num curto espaço de tempo, vão ser submetidos no mercado produtos com novos mecanismos de defesa. Se contabilizarmos de tempo, a utilização destes mecanismos pelos atacantes não serve mais do que para primeiro orquestrarem, e depois fazer uma redução substantiva do tempo. Se utilizarmos os métodos tradicionais, será completamente impossível colmatar seja o que for deste tipo de ataques".

Paulo Pinto (Fortinet) diz que "no contexto das infraestruturas digitais e no posicionamento no ciberespaço, as pessoas, por si próprias, não vão ser capazes de lidar com a quantidade de alertas que vão chegar dos diversos sistemas. De uma forma muito simples, a automação e o machine learning vão ter um papel primordial no apoio às equipas de cibersegurança. A forma como vai ser aplicado exige cuidado porque estes algoritmos precisam de uma grande quantidade de dados para que possam produzir informação prática".

David Grave (Claranet) explica que "é necessário esse poder de computação para analisar a quantidade e a qualidade dos dados. Podemos treinar os elementos cognitivos, mas são precisos dados de qualidade. Isto é crítico. Para os clientes mais pequenos, é preciso dar acesso a esse poder de computação para ter acesso a uma enorme quantidade de dados que o cliente, de outra forma, não teria. A inteligência artificial é um serviço para os analistas altamente especializados que vão passar a ter informação de qualidade para trabalhar".

TENDÊNCIAS PARA 2021

Com um mundo em constante mudança, muitas são as tendências que existem à volta dos sistemas de informação. Na cibersegurança não é exceção e as organizações devem adaptar-se a novas realidades neste segmento.

Nuno Cândido (Noesis) refere que "se vai dar continuidade à adaptação à realidade de teletrabalho e são esperados investimentos em soluções empresariais para dar resposta a este novo paradigma. Creio que as PME vão ter de aumentar bastante o investimento em cibersegurança; muitas delas tiveram de aumentar a sua exposição online e o segundo passo é começarem a sofrer ataques, perdas de negócio, e terão de começar a ter muita atenção à questão da segurança".

Alexandre Costa (Nexllence) explica que "as principais tendências continuam a ser os ataques de ransomware, de DDOS e de *Advanced Persistent Threats*. A dark web irá permitir cada vez mais aos cibercriminosos aceder a dados sensíveis de redes das organizações. Acho que vão continuar a existir cada vez mais produtos e serviços de segurança que vão trazer uma gestão mais complexa às corporações. Depois, as próprias fusões e aquisições nesta área vão ser uma tendência nos próximos anos".

- Nuno Cândido, Noesis -

- Carla Zibreira, S21sec -

José Borges Ferreira (Anubis Networks) menciona que, "ao longo dos anos, a evolução de classificação de eventos foi interessante. Passámos da evolução simples, para a classificação com machine learning com base nos dados recolhidos, para as redes neurais onde já não é preciso um grande *data set* de treino. São estes algoritmos que nos vão permitir tomar decisões para algo que não conhecemos. Estamos a tentar prever o que vem por aí, mas devemos estar preparados para o que não conhecemos".

- Bruno Gonçalves, Warpcom -

FOCO NO *ENDPOINT*

Élio Oliveira (Kaspersky) afirma que "é preciso haver um foco no *endpoint*, e não falamos apenas na componente do antivírus, mas numa componente mais avançada como a resposta automática a incidentes, o vulgo EDR. Depois, também é preciso consciencializar os utilizadores, o *awareness*, para os perigos da cibersegurança. A autenticação multifator e o acesso à cloud vão ser tendências no mundo da cibersegurança nos próximos anos".

Fernando Cardoso (Layer 8) indica que "as tendências para 2021 vão estar intimamente ligadas à pandemia e ao paradigma de teletrabalho. Vão acontecer mais ataques nos computadores e redes domésticas, onde os criminosos vão utilizar esses equipamentos para saltarem para as redes empresariais ou para as clouds onde os utilizadores estão ligados. Terá de existir, necessariamente, um investimento maior na segurança do *endpoint*, dos EDR e em abordagens *zero trust*".

Bruno Gonçalves (Warpcom) diz que "este ano vamos continuar a assistir e o foco será criar mais resiliência. As organizações vão estar focadas em criar mais resiliência nas suas infraestruturas que toca em vários pontos: no *awareness* dos colaboradores, num maior controlo dos processos, nos *endpoints* e na gestão de identidades. Por último, é a questão das redes quânticas que vai trazer uma nova realidade e uma nova capacidade para os atacantes".

Carla Zibreira (S21sec) refere que "a pandemia veio transformar a forma como as organizações fazem aquilo que é o seu negócio e, como tal, há uma maior exposição por parte desses processos à Internet. Aí, o *compliance* – ao contrário do que inicialmente se podia pensar – não aligeirou e as reguladoras continuaram atrás das empresas, a exigir o cumprimento dos *timings*, a certificação ou a entrega de evidências de cumprimento em relação a um *framework*. Quando falamos em segurança também falamos em confiança; quando viramos o negócio para o exterior, essa é a palavra-chave". ■

- Bruno Gonçalves -
Business Unit Manager – Cybersecurity & Public Safety, Warpcom

"Todos os dias nos deparamos com ataques mais sofisticados com um impacto brutal para as organizações"