O Jornal Económico

ESPECIAL

Cibersegurança

EMPRESAS VÃO CONTINUAR A INVESTIR EM CIBERSEGURANÇA

Conheça as previsões da consultora IDC para a cibersegurança em Portugal. As áreas que deverão ter mais crescimento são Software de Gestão de Acessos Privilegiados (19,5%) e Managed Security Services (18,9%). Leia ainda a entrevista exclusiva à especialista Miri Marciano, que trabalhou mais de 20 anos na segurança informática das Forças Armadas do Iraque e faz agora parte da BCG.

ANÁLISE

Investimento na cibersegurança vai superar os 411 milhões de euros este ano

A área que deverá crescer mais em Portugal é a de software de gestão de acessos privilegiados, de acordo com as previsões da consultora IDC.

MARIANA BANDEIRA
mbandeira@medianove.com

As organizações portuguesas vão investir cerca de 300 milhões de euros em soluções de segurança informática este ano, o que representa um aumento homólogo de 10,7%, adiantou esta quinta-feira a consultora International Data Corporation (IDC), no relatório mais recente de previsões tecnológicas.

Os analistas da IDC antecipam que as áreas da cibersegurança que vão crescer mais segurança em Portugal em 2023, são Software de Gestão de Acessos Privilegiados (19,5%); *Managed Security Services* - ou serviços de segurança geridos, na tradução à letra - (18,9%); Deteção e Prevenção de Intrusão (17,5%); Software de Avaliação de Vulnerabilidades de Dispositivos (16,7%); Software de Gestão de Identidade (16,4%); Software de Segurança de Aplicações Ativas (15,4%) e Software de Gestão de Dados Sensíveis e Privacidade de Dados (15,4%).

"Será inevitável a ocorrência de ciberataques graves nos próximos anos. Como tal, todas as organizações deverão migrar de um foco exclusivo em segurança cibernética para um conceito de resiliência cibernética organizacional. A abordagem passa por assumir que os incidentes vão acontecer e preparar para recuperar a continuidade operacional e do negócio o mais rapidamente, com o mínimo de impacto na organização", começa por explicar Adaíl de Oliveira, responsável de Managed Security Services da Cipher na região da Europa, África e Médio Oriente.

Para o executivo da Cipher, a empresa que reúne as atividades da Prosegur na cibersegurança, "é essencial que as organizações estejam atentas à exposição dos seus ativos, monitorizem alterações súbitas de comportamentos seja de dispositivos ou de atividades relacionadas com os utilizadores", bem como "apostar em plataformas unificadas que promovam a visibilidade contínua de todos os ativos das organizações e que permitam cobrir todas as superfícies de ataque", nomeadamente infraestruturas de Tecnologias da Informação (TI), Tecnologia Operacional (TO), Internet das Coisas (IoT - Internet of Things) ou armazenamentos na nuvem (*cloud*).

João Cupertino
Head de Cibersegurança da Pamafe (Ricoh)

Gonçalo Caseiro
Consultor

Adaíl de Oliveira
Head de 'Managed Security Services ' da Cipher na EMEA

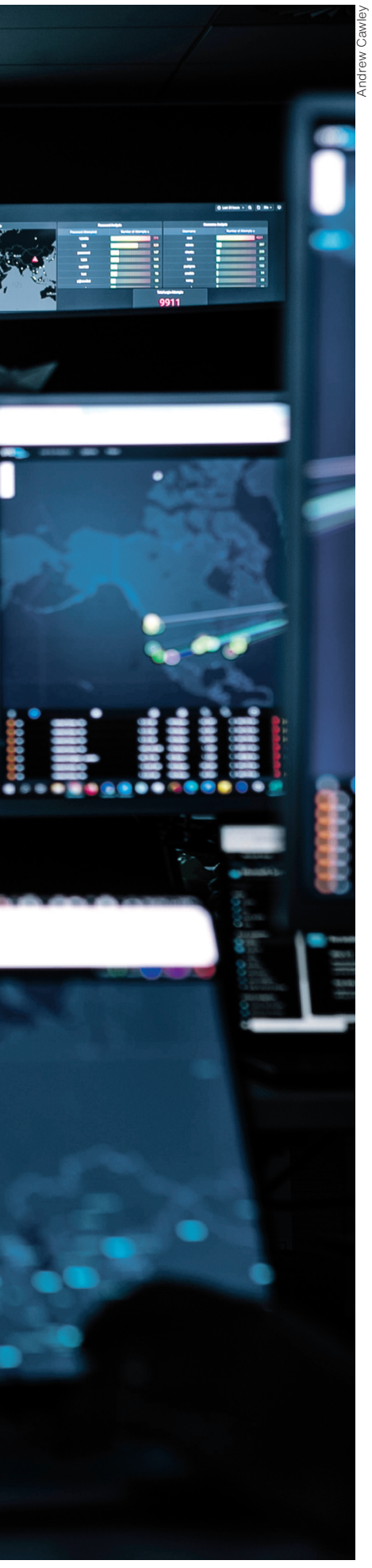
"A parte física e a parte digital são pouco ou nada tolerantes a falhas. Quando um operador de telecomunicações em Portugal teve um problema grave e o INEM deixou de funcionar percebeu-se que o sistema não era tolerante a falhas. Quando os correios do Reino Unido sofreram um ataque de *ransomware*, no início deste ano, constatou-se que os pequenos negócios não conseguiam funcionar e enviar as suas encomendas", afirma Gonçalo Caseiro, consultor e especialista em inovação e transformação digital, ao Jornal Económico (JE).

As últimas previsões da IDC para a área da cibersegurança apontam para que, até 2026, um terço (30%) das grandes empresas pretendem migrar para centros de operações de segurança autónomos, acedidos por equipas distribuídas, para gerar uma mitigação mais rápida, e uma melhoria da resposta e da gestão de incidentes. Mais: daqui a dois anos, quase metade (45%) dos CEO vão exigir métricas de segurança e medição de resultados para avaliar e validar investimentos feitos no programa de segurança, bem como prever o retorno do investimento (ROI - Return Over Investment).

"A evolução de soluções que garantem a resiliência das instituições é, cada vez mais, uma preocupação dos clientes, o que reflete a crescente procura de soluções resiliência e a segurança e a sua aquisição", garante Bruno Mendes, da Dell Technologies Portugal. AO JE, o executivo sénior de vendas na área de Proteção de Dados assegura que "os clientes mostram grande interesse em proteger *backups* contra ransomware, onde a terminologia sobre *air gapping* e imutabilidade é frequentemente confundida". "No entanto, a implementação destas soluções desperta maior interesse do sector financeiro, cuidados de saúde e sector público, que são mais regulados, enquanto outras indústrias estão a analisar ou a implementar versões mais simplificadas", clarifica o porta-voz nacional da tecnológica norte-americana, que no mês passado lançou soluções neste ramo, inclusive o Managed Detection and Response Pro Plus, para bloquear acessos a *hackers* e acelerar a recuperação de ataques, ou o CrowdStrike, ligado à gestão de ameaças em *endpoints*, redes e *cloud*.

Negócio de cibersegurança representa 8% do negócio da Ricoh em Portugal

A multinacional japonesa Ricoh, de produtos de eletrónica e


Andrew Cawley

software, prevê um "forte crescimento" do negócio da cibersegurança em Portugal, que atualmente representa neste momento cerca de 3,9 milhões de euros, ou seja, 8% da faturação total da Ricoh no país.Em Portugal, esta área do grupo com sede em Tóquio registou um crescimento de 79% no último ano.

"Esperamos continuar a crescer de forma sustentada nos próximos tempos. O nosso portefólio de serviços por ser bastante abrangente e completo tem levado ao crescimento do número de novos clientes em cerca de 40%. Há ainda que referir que cerca de 60% dos nossos clientes expandiram a abrangência dos serviços contratados connosco", avançou ao JE o responsável de Cibersegurança da Pamafe (Ricoh Company).

"Existe uma grande visibilidade na comunicação social sobre os ataques cada vez mais frequentes, o que conjugado com a maior pressão regulatória, nacional e internacional, leva as organizações a investir no aumento do grau de maturidade, demonstrado em particular pelo crescimento dos serviços de auditoria e apoio na implementação das medidas de controlo e governação da arquitetura de segurança. No entanto, não há sinais de que os cibercriminosos vão desacelerar as suas ações a médio prazo. É, por isso, fundamental assegurar as medidas necessárias de proteção", advertiu João Cupertino.

O fundador da GConsulting, Gonçalo Caseiro, diz que a chave para o sucesso também está no investimento na formação das pessoas e na sensibilização de qualquer trabalhador de uma empresa, à semelhança do que tem vindo a ser dito pela generalidade dos peritos na área. "Os investimentos em muita tecnologia não se sobrepõem a esta necessidade, porque as falhas dos humanos são o principal vetor dos ciberataques", argumenta o ex-consultor da Accenture e antigo administrador da Agência para a Modernização Administrativa.

Gonçalo Caseiro lembra que o número de denúncias ao gabinete de cibercrime da PGR aumentou 113% em 2021, mas o número de arguidos relacionados com estas matérias de informática reduziu 36%, de 2019 para 2020. "Apesar de estar a haver mais ataques, tornam-se mais difíceis de identificar, porque são mais complexos e é mais complicado perceber realmente o que é que aconteceu. A complexidade parece não estar a permitir que as entidades consigam atuar", afirma, acrescentando que o Centro Nacional de Cibersegurança tem feito um bom trabalho em criar perceção pública para estes riscos, tanto na gestão das instituições do Estado como nos cidadãos comuns.

Todavia, o estigma de ser alvo de ataques mantém-se – sobretudo pelos danos reputacionais – mas é algo que terá de mudar rapidamente. Para Gonçalo Caseiro, é uma questão de entreajuda das organizações para prevenção dos cidadãos. "Seguramente, os ciberataques só vêm a público e são confirmados pelas empresas quando é demasiado evidente para os clientes [que houve um ciberataque]. Existe relutância em revelar que há dados vulneráveis. Isto vai ter de mudar porque se as empresas tiverem responsabilidade - agora cumprirem a lei – e informarem de que forma os seus sistemas foram vulneráveis vão auxiliar outras a protegerem-se", explica o ainda assessor da administração da AlmaScience e membro do conselho geral da AESE Business School. ■

Breves

Comissão Europeia reforça cooperação entre Estados-membros

A Comissão Europeia adotou esta terça-feira uma proposta de ato legislativo da União Europeia (UE) sobre cibersolidariedade destinado a reforçar as capacidades da UE no domínio da cibersegurança. Esta decisão deverá contribuir para melhorar a deteção e a sensibilização para ameaças e incidentes de cibersegurança, apoiará a preparação das entidades críticas e reforçará a solidariedade, a gestão concertada de crises e as capacidades de resposta em todos os Estados-membros. O ato legislativo sobre cibersolidariedade cria capacidades a nível da UE de forma a tornar a Europa mais resiliente e mais reativa face às ciberameaças, reforçando simultaneamente o mecanismo de cooperação existente.

Allurity compra empresa portuguesa CloudComputing

O grupo sueco Allurity, fornecedor de serviços de cibersegurança, concluiu esta semana a aquisição da empresa portuguesa CloudComputing, por um valor que não foi revelado ao mercado. O negócio foi feito através da Trill Impact, fundo private equity apoiado pela Nordea Asset Management, uma das maiores empresas de gestão de ativos dos países nórdicos.
Fundada em 2010, a CloudComputing gere mais de 10 milhões de identidades digitais. Além disso, trabalha em domínios como gestão de identidades, jornadas *zero trust, digital workplace* e *mobile security*. Com esta operação, a Allurity acredita que está a dar impulso à estratégia de crescimento em mercados chave, como a Bélgica, os Países Baixos e o sul da Europa. Em 2022, a Allurity teve um volume de negócios consolidado de mais de 70 milhões de euros e prevê atingir os 250 milhões nos próximos dois anos. Para tal, tem vindo a realizar uma série de aquisições.

'Phishing"com criptomoedas sobe 51%num ano

O phishing, técnica de fraude eletrónica para obtenção de dados confidenciais, direcionado para o roubo de criptomoedas aumentou 40% no ano passado, segundo a Kaspersky. A empresa de antivírus concluiu que houve 5.040.520 deteções em 2022, mais do que as 3.596.437 no ano anterior. "Este aumento poderia ser parcialmente explicado pelo caos que ocorreu no mercado de criptomoedas no ano passado. Um em cada sete utilizadores de criptomoedas foi afetado por phishing", explicaram os especialistas da marca russa. Portanto, antes de investir em qualquer moeda virtual, investigue a plataforma e respetivos website, redes sociais e equipa para garantir que é legítima, sugerem.

ENTREVISTA | MIRI MARCIANO | Especialista em cibersegurança da Boston Consulting Group

"Hoje os cibercriminosos têm planos, I&D e orçamentos"

Miri Marciano, especialista em cibersegurança da consultora BCG, afirma que os "agentes das ameaças" informáticas fazem parte de autênticas empresas que conseguem saber onde estão os alvos que lhges gerarão receitas.

MARIANA BANDEIRA
mbandeira@medianove.com

Miri Marciano, especialista de cibersegurança da Boston Consulting Group (BCG) e diretora associada da consultora em Telavive, deu uma entrevista exclusiva ao Jornal Económico (JE) aquando da sua última visita a Lisboa, a 29 de março. A antiga oficial de Tecnologia e Cibernética nas Forças de Defesa de Israel, para onde trabalhou durante mais de duas décadas, diz ao JE que há casos de ataques informáticos em que "não se consegue entender logo qual é a motivação está por trás. "Pensa-se que é financeira, porque pedem dinheiro, mas por trás está o apoio de uma nação", alerta.

Escreveu um artigo com previsões de cibersegurança para este ano. Porque é que acha que o ransomware continuará, novamente, em primeiro?
Porque é a maneira mais fácil de ganhar dinheiro. Tornou-se muito simples ativá-lo, dado que existem muitas vulnerabilidades nas organizações que os criminosos podem utilizar. Eles são criminosos bem preparados. Já não é apenas *hacking* nalgum lugar, alguém sozinho ou um grupo de *geeks*. Nada disso. Na verdade, são empresas bem estabelecidas, com I&D [Investigação e Desenvolvimento], que criam ferramentas, têm as suas finanças e um plano de trabalho e estão, cada vez mais, a ganhar conhecimentos para entender que tipo de organizações lhes pode ser relevante e gerar receita.

> **Isto é uma selva e uma corrida. Se fores mais rápido a criar recursos do que os outros, serás mais rápido a proteger-te. Se fores mais lento ou mesmo o mais fraco ficarás mais vulnerável**

Como é que começam o ataque?
Fazem um exercício de dentro para fora para entender a partir de onde é que podem entrar [na rede de uma empresa]. Dizem algo do género: "Ok, esta organização é muito fraca nos controlos de prevenção. Então, talvez possamos começar com uma campanha de *phishing*", para os trabalhadores entrarem nos *links*. A maneira mais fácil é começar com o fator humano. É engenharia social.

Entrou há cerca de dois anos na BCG. O que nos pode dizer sobre o tipo de projetos nos quais está envolvida?
Como empresa de consultoria estratégica, estamos a ajudar os nos-


Cristina Bernardo

sos clientes a reconstruir-se ou a entender aquilo de que precisam para lidar com os riscos cibernéticos. Levar estes temas para os conselhos de administração, desenhar uma estratégia de cibersegurança feita à medida da sua organização, perceber como podem medir e gerir o risco para saberem onde precisam de investir, qual é o lugar certo – em que recursos – em que devem colocar o dinheiro.

A vossa equipa defende que, nessa estratégia de cibersegurança, não é preciso ser o melhor da turma, mas pelo menos ter um negócio com aptidões fortes...
Isto é como uma selva. Precisas de correr mais rápido do que os teus pares, porque vai ser mais fácil para os agentes das ameaças agarrarem a cadeia mais fraca que conseguirem. Portanto, se fores mais rápido a criar recursos do que os outros, serás mais rápido a proteger-te. Se fores mais lento ou mesmo o mais fraco ficarás mais vulnerável. É uma corrida.

É por essa razão que diz que "os dias de tratar a cibersegurança como uma reflexão futura ou um complemento (*add-on*) acabaram há muito tempo"?
Há mais e mais ataques e parte deles são muito massivos e trazem muitos prejuízos para as empresas. Há aqui várias motivações. Primeiro, os criminosos querem dinheiro, então vão trabalhar para atingir esse objetivo. Segundo, a motivação geopolítica, que é diferente, porque os cibercriminosos querem criar confusão numa comunidade. Às vezes, não se consegue entender logo qual é a motivação está por trás do ataque. Pensa-se que é financeira, porque pedem dinheiro, mas por trás está o apoio de um estado-nação.

Pedem dinheiro para tentar esconder ambições maiores?
Exatamente.

Pouco depois de assumir estas funções, eclodiu uma guerra na Europa. Acha que a invasão russa trouxe mais consciência sobre o risco geopolítico no mundo digital?
A guerra foi um dos marcos nesta atmosfera do ciberespaço. Hoje, o online é uma espécie de arma que os governos usam para a guerra e, às vezes, em paralelo com as outras. Tens as bombas e também tens as bombas digitais. Vimos vários exemplos disso, que criaram mais consciência – nas empresas e nos países em todo o mundo, especialmente na Europa - de que algo pode realmente acontecer. O segundo ponto de mudança, antes, foi a Covid-19. O que é que aconteceu durante a pandemia? Uma completa loucura no mundo que causou impacto em muitas coisas. As pessoas estavam sentadas em casa e os criminosos também estavam nas suas casas, com muito tempo para atualizar os seus modelos operacionais. Havia muita vulnerabilidade nas redes e tornava-se muito fácil utilizá-las para ganhar dinheiro.

Qual é a sua opinião sobre a regulação na União Europeia? Depois do DORA, até outubro de 2024 os Estados-membros têm de transpor as diretivas SRI2 e REC.
Os reguladores começaram, de facto, a colocar as exigências para estruturar e controlar a loucura que estava a acontecer [com a Covid-19]. O DORA [Digital Operational Resilience Act] é um desses exemplos. Vemos que também outros países estão a tentar incorporar uma espécie de requisitos e recomendações. Às vezes começa como uma recomendação e depois torna-se um regulamento com cumprimento de *compliance* e assim por diante. Por exemplo, na Singapura ou nos Estados Unidos, onde Biden declarou a necessidade de requisitos específicos para infraestruturas críticas.

Então e qual é o papel do CEO neste processo?
Boa pergunta, porque acho que ainda temos muitos CEO que pensam que a cibersegurança não faz parte da sua liderança e das suas decisões de investimento. Acho que quando o tempo passar e tivermos muitos ataques bem-sucedidos, que prejudicam as organizações e seja tudo divulgado – a regulação vai obrigar a declarar e no passado as organizações escondiam, por não ser bom para os acionistas e *stakeholders* – deixa de ser uma vergonha.

Qual a principal aprendizagem que ficou do seu percurso profissional em instituições de defesa de Israel?
Estive 25 anos nas Forças Armadas israelitas nas unidades de tecnologia e ciberespaço. Comecei como programadora, depois líder de projeto, chefe de equipa de engenharia e assim por diante. Talvez há doze anos, esta questão da cibersegurança tornou-se um tópico real, que precisávamos de começar a endereçar ao nível das indústrias da defesa. Então, comecei a minha carreira a perceber que o domínio cibernético faz parte das entidades de defesa e depois, há cerca de seis anos, continuei na área, mas em instituições públicas, como a Direção Nacional Cibernética de Israel [Israel National Cyber Directorate], e no sector privado.

Uma espécie de supervisor nacional de cibersegurança?
Sim. É uma agência cibernética, que no fundo está a criar capacidades para ter mais cibersegurança no país e para criar relações de cooperação. Hoje vemos que muitos países já criaram este tipo de entidades, tal como aqui em Portugal. Basicamente, destina-se a trazer capacidades para a nação que também podem ser muito relevantes para as organizações, de grande dimensão ou PME, e mesmo para as pessoas, para os cidadãos. Eu fazia parte dessa entidade em Israel e a minha função lá era a chefia das operações cibernéticas, o que significa que estava encarregada de proteger as infraestruturas críticas.

É mais fácil proteger instituições do Estado ou os privados?
Depende da função que se tem em cada uma. Quando comecei a trabalhar no âmbito de uma nação, existiam as capacidades mais avançadas, as oportunidades, os desafios que trazem os agentes de ameaças. Como vemos, também noutros países, não só em Israel, demora algum tempo até os ataques começam a penetrar, então por vezes os governos são os primeiros a tentar reagir ou perceber o que fazer no país e, depois, tentar criar diretrizes e *frameworks*. A inovação não é uma guerra, mas a estrutura da situação a nível nacional, envolve tentar perceber "o que vamos fazer com este tipo de ameaça?". Levei esse ponto de vista para o privado, para tentar melhorá-lo e especificá-lo.

O que a traz a Portugal?
Tivemos um evento onde reunimos com vários CEO e *C-Levels* a quem colocámos em cima da mesa, a compreensão sobre as ameaças e os desafios que as organizações hoje enfrentam. Como é que uma empresa reage? Que tipo de capacidades, normalmente, precisa de criar para se proteger? ■

JE TALKS

Fator humano já não é necessário aos ataques

A evolução da tecnologia é tal que os ataques são feitos de forma cada vez mais sofisticada e cada vez mais difícil de detetar, ao mesmo tempo que as medidas de prevenção são cada vez mais fortes, alertam especialistas.

TOMÁS GONÇALVES PEREIRA
tpereira@medianove.com

Todas as empresas correm o risco de serem alvo de ataques cibernéticos, na atualidade. Os atacantes recorrem às tecnologias mais recentes para que consigam ultrapassar defesas mais resistentes, de forma a poderem aceder a dados que estão mais bem protegidos. Capacitar as companhias e respetivas plataformas digitais para poderem resistir a este tipo de ofensivas é o principal propósito de empresas como a Visionware.

O fundador e CEO da companhia, Bruno Castro, sublinhou na JE Talks desta semana que os gestores estão agora em alerta para este tipo de ameaças, já que se registam múltiplos casos todas as semanas. Inclusive, atualmente, as questões de teor cibernético fazem parte da "estratégia" das empresas, refere.

As mesmas empresas já aplicam, inclusive, uma parte dos orçamentos concretamente a este tipo de proteção, mas trabalhar num processo de evolução constante é de elevadíssima importância, já que as tecnologias utilizadas pelos atacantes também se tornam cada vez mais capazes de entrar em bases de dados mais evoluídas, já que se tornam cada vez mais difíceis de detetar.

Aliás, o mundo digital deu "um salto gigantesco, muito maior que as pernas" devido à pandemia e, por esse motivo, vão surgir "cogumelos digitais". O aparecimento de novas tecnologias e soluções interativas vai trazer diversas vantagens, mas vai também gerar dificuldades na gestão das mesmas.

A chegada em força do 5G vai levar a que os dispositivos que usamos passem a estar interligados, o que significará "alargar brutalmente" a superfície de ataque.

Porém, já que os avanços tecnológicos permitem e vão continuar a permitir, maior sofisticação ao nível das defesas, também os ataques se vão tornar mais evoluídos e, por esse motivo, mais perigosos. Os piratas informáticos que operam mega-ataques trabalham, por norma, em "consórcios" e o seu objetivo passa por conseguir aceder à rede das empresas sem serem detetados, como explica Bruno Castro.

Os mecanismos atualmente são de tal forma evoluídos que já é possível realizar estas ofensivas sem usar o fator humano, bastando agora recorrer à vertente digital.

Este progresso representa novos perigos, não apenas para as empresas, mas também para as instituições estatais que, no caso de não terem mecanismos de defesa suficientemente sólidas, pode deixar comprometida a integridade dos países.

"O que temos vindo a ver constantemente é que há várias ondas sucessivas de ataques direcionados tipicamente às pessoas, personas e às empresas e advém de várias motivações", sublinha o responsável, que lembra que quando as defesas não são capazes de contrariar as

ofensivas, os dados intercetados pelos atacantes podem ficar comprometidos.

A CheckPoint Software Technologies especializa-se em tecnologias de defesa contra ataques cibernéticos. O country manager em Portugal, Rui Duro, destaca que os ataques acontecem com grande frequência e, em Portugal, a proporção é similar à de toda a Europa, independentemente da localização geográfica do país na ponta oeste do continente.

"Não há uma geografia no canto da Europa que nos proteja", reitera, esclarecendo que Portugal está diretamente ligado aos outros Estados "no mundo virtual, no mundo completamente conectado". Neste contexto, os ataques são de tal forma evoluídos e potencialmente direcionados a organizações em Portugal, que o responsável lembra que a sua empresa não apenas desenvolve produtos, como também realiza investigação sobre as novas funcionalidades existentes, o que se revela fundamenta para responder às ameaças com que a empresa se depare no futuro.

Como explica o responsável, essa investigação é essencial para obter informação sobre novas metodologias, por exemplo, de forma a perceber que tipo de ataques se podem estar a aproximar, o que se pode revelar essencial para que a resposta dada seja suficiente para neutralizar o ataque ou, pelo menos, reduzir o impacto do mesmo. Ao mesmo tempo, a evolução ao nível dos métodos dos atacantes é evidente como explica Bruno Castro.

No caso do phishing, o progresso passa por tornar cada vez mais difíceis de detetar as hiperligações que têm como finalidade roubar os dados pessoais dos utilizadores. Desde a documentação pessoal aos cartões bancários, as metodologias utilizadas refletem um progresso cada vez maior no plano das tecnologias. Uma tendência de sofisticação que se vai manter no futuro, tal como acontece com os ataques de ransomware.

Esta modalidade de ataque já não serve unicamente para roubar dinheiro. Agora é já possível utilizá-lo com uma plataforma de cibercrime altamente sofisticado, de forma que os métodos para enganar os utilizadores se tornem cada vez mais indecifráveis.

Simultaneamente, cabe a empresas como a Check Point e a VISionWare desenvolver tecnologia que ajude os utilizadores, as empresas e as instituições estatais a defenderem-se contra as ameaças. De acordo com o responsável, existem ainda outros riscos associados. A própria funcionalidade 5G traz as mais variadas vantagens à sociedade, mas representa também algumas ameaças. Ora, o capítulo das ameaças cibernéticas não foge a estes riscos. É que a chegada em força da rede móvel de quinta geração vai levar a que os dispositivos que usamos passem a estar interligados, o que permitirá "alargar brutalmente" aquilo que é conhecido como a superfície de ataque.

Bruno Castro recorda ainda que, no âmbito da guerra entre a Rússia e a Ucrânia, os ucranianos cedeu uma série de "armas cibernéticas" a um exército daquela área constituído por pessoas que não têm know-how suficiente para lidar com tais ferramentas, que são sinónimo de grande capacidade e, por consequência, de grande responsabilidade

CAIH, a nova associação de segurança digital

Esta quinta-feira o Governo aprovou em Conselho de Ministros o decreto-lei que cria a associação sem fins lucrativos Cyber Academia and Innovation Hub (CAIH), de direito privado, cuja missão é promover e realizar atividades de interesse público nas áreas da cibersegurança e da ciberdefesa e suas interfaces com outras políticas sectoriais.

"A CAIH concretiza a execução de um projeto PESCO liderado por Portugal centrado na formação, treino e exercícios, investigação, desenvolvimento e inovação, bem como no desenvolvimento industrial, em estreita colaboração com os organismos da administração pública, instituições de ensino superior e tecido empresarial", defendeu o Executivo liderado por António Costa, em comunicado após a reunião de ministros. ■

CIBERSEGURANÇA E IMUNIDADE DE GRUPO

Na cibersegurança, para que uma comunidade se torne resiliente a abordagem à gestão do risco de terceiros torna-se extremamente relevante, da mesma forma que o risco de doença desaparece quando não consegue contaminar um grupo de pessoas, também uma brecha num determinado sistema informático não se espalha quando as entidades em seu redor estão seguras.

Em cibersegurança, este conceito dá pelo nome de Third Party Risk Management (TPRM), mas, a sua implementação ainda está muito condicionada pela mentalidade do "eu versus eles", que torna esta resiliência de grupo difícil de alcançar. Isto é, ainda há entidades terceiras a reagir tardiamente aos desafios da cibersegurança e, se falarmos de "quartas entidades", é provável que nestas o tema da cibersegurança esteja a ser totalmente ignorado.

Habitualmente, as empresas tendem a assumir que o risco de terceiros pode ser gerido a partir do conjunto de dados que é partilhado ou através da gestão e controlo da sua sensibilidade. De facto, apesar de essa ser uma medida higiénica do ponto de vista da cibersegurança, a verdade é que uma eventual violação de dados aparentemente inócuos pode infetar e alastrar rapidamente ao ecossistema de parceiros e exponenciar o impacto noutras áreas e sistemas.

Para evitar isso, é mandatório fazer uma abordagem ao ecossistema, reorientando a cibersegurança para o conceito TPRM, ou seja, em torno de um "nós" coletivo.

A abordagem ao "nós" coletivo

A abordagem ao "nós" coletivo em cibersegurança cruza uma linha, por vezes, invisível, que separa uma empresa dos seus parceiros e é uma abordagem bastante exigente se tivermos em consideração que apenas 53% das empresas afirmam confiar plenamente na cibersegurança dos seus parceiros[1]. Por outro lado, avaliar os problemas de segurança dos parceiros pode não ser uma tarefa fácil e as autoavaliações correm o risco de não serem credíveis se não forem validadas por uma entidade independente. Neste caso, o problema não é tanto a natureza paternalista de muitas abordagens, mas a suspeição que levanta acerca da eventual pouca confiabilidade das medidas implementadas pela empresa parceira.

Além disso, algumas empresas, principalmente as de menor dimensão, enfrentam muitas vezes o dilema sobre o tipo de investimento que devem fazer para se manterem competitivas. Isto é, se investem em tecnologia produtiva ou se investem em cibersegurança[2].

Diferentes indústrias enfrentam, também, diferentes desafios. Na prática, trata-se de uma equação em que reduções marginais no risco podem não justificar aumentos substanciais nos investimentos e, portanto, tudo se resume a um equilíbrio entre as duas escolhas.

1 "The modernization of cybersecurity: How technology is changing the way businesses view vendor assessment and cybersecurity." Whistic & RiskRecon (a Mastercard company), 2022."

2 "Water under the breach: The sunk costs of cyber security." Mastercard, 2019

Incrementar a ciber resiliência

O facto incontestável é que a digitalização, os negócios em rede e as ameaças à segurança transformaram monólitos corporativos em borboletas sociais e a abordagem TPRM prepara estas "borboletas" para saberem gerir a sua distância social.

Em suma, a aplicação do TPRM é uma tarefa difícil, porque uma empresa não pode funcionar adequadamente e permanecer completamente protegida quando as suas expectativas em relação à cibersegurança das empresas com quem se relaciona é baixa. Também não se pode esperar que uma determinada empresa parceira possa alcançar determinadas expectativas quando as soluções de cibersegurança disponíveis não respondem a uma framework independente pensada para responder ao desafio do "nós".

Em suma, a cibersegurança existe para fortalecer componentes vulneráveis de determinadas empresas contra eventuais incidentes e esse é o nosso principal foco. E só através de uma visão holística de todos os negócios envolvidos num determinado ecossistema é possível suavizar o impacto das violações dos sistemas e incrementar a ciber resiliência.

Nos últimos 5 anos, a Mastercard investiu cerca de mil milhões de euros em recursos de cibersegurança e contribuiu para o lançamento de mais de 20 startups com soluções inovadoras para cibersegurança.

O conjunto de ferramentas de cibersegurança da Mastercard, que vão desde a quantificação de riscos, por meio de simulações de violação e ataque, à abordagem TPRM, asseguram a resiliência das empresas, dos seus ecossistemas e são uma solução para responder ao desafio da imunidade digital de grupo. Saiba mais em:

https://www.mastercardservices.com/en/solutions/cyber-security-risk

FÓRUM

Um orçamento individual sem magia pensado para salvaguardar as contas

Mais vale prevenir que remediar. O Jronal Económico falou com empresas que dizem não existir uma percentagem fixa quando se fala no orçamento a alocar à cibersegurança, embora este deva cobrir todos os riscos.

Qual a percentagem que as empresas devem alocar do seu orçamento para a área de cibersegurança? INÊS FILIPA MIGUEL

RICARDO NEGRÃO
Head of Cyber Risk da Aon em Portugal

Mais que o valor para o orçamento de cibersegurança é importante saber o ponto de partida, isto é, qual o nível de maturidade para este risco, pois o valor a orçamentar será diferente estando numa maturidade mais baixa ou mais elevada. A avaliação de risco cibernético permite às empresas identificarem onde se encontram e definir um plano de melhoria onde mitigam as vulnerabilidades com a implementação de controlos adequados.

Além do ponto de partida, consideramos que existem outros fatores que afetam o valor percentual do orçamento e que devem ser avaliados. Por exemplo, a dependência tecnológica do nosso negócio tem um impacto na percentagem alocada, pois quanto maior for a sua dependência tecnológica maior é o risco e a necessidade de elevar a maturidade de cibersegurança, e com isso ter orçamentos superiores. Outro fator está relacionado com o tipo de informação que gerimos, se é sensível, confidencial, propriedade intelectual, dados pessoais e que faz variar os controlos de segurança a implementar perante os riscos e impactos identificados.

A nossa visão é que não se deve dissociar a segurança física da segurança tecnológica, isto é, a segurança deve ser olhada como um todo e não ser separada do ponto de vista organizacional nem orçamental, uma vez que uma vulnerabilidade na segurança física pode originar impactos significativos. Por exemplo, numa instalação industrial onde existam falhas nos controlos de acesso físico aos ativos da tecnologia industrial podem facilitar uma instrução na rede industrial, mesmo sem a mesma estar liga à internet.

Tendo em conta esta nossa visão defendemos que as organizações devem alocar 5% a 10% do seu orçamento de IT, variando este valor dos fatores acima identificados.

E por fim, dar uma última nota que existe outra componente relevante nos controlos deste risco que nunca está alocado aos orçamentos de IT, nem de cibersegurança que é o risco dos seguros, onde o investimento num seguro para o Risco Cibernético representa um investimento significativo, mas é uma forte proteção em termos do impacto financeiro que os incidentes de segurança originam.

DAVID GRAVE
Diretor de Cibersegurança na Claranet

Para as empresas, o investimento na cibersegurança deverá ser uma preocupação crucial. A não alocação de recursos de ciberproteção pode deixar uma organização vulnerável a ataques de vários tipos, resultando, com grande probabilidade, em danos computacionais, financeiros, legais e reputacionais.

Existe, entre os fabricantes e fornecedores de soluções de proteção digital, um consenso relativo à recomendação de as empresas reservarem entre 5% e 15% das suas receitas para investimentos em cibersegurança.

Contudo, o orçamento que uma organização deve atribuir à cibersegurança não é fixo e depende de vários fatores, como a sua dimensão, complexidade do negócio ou a área de atuação.

É também importante assumir que o investimento em cibersegurança, hoje, deverá ser diferente daquele que era realizado há alguns anos.

Além de investir em tecnologias de proteção inteligente dos dispositivos, das aplicações e das infraestruturas utilizadas, há que considerar o investimento no conhecimento e na consciencialização dos colaboradores – eles tornaram-se num fator decisivo, de primeira linha, para a proteção dos sistemas e da informação das organizações.

Dependendo dos requisitos e dos recursos disponíveis, algumas organizações poderão necessitar de investir substancialmente mais em cibersegurança, enquanto outras podem afetar menos recursos.

RUI SHANTILAL
Managing Partner da Integrity part of Devoteam

A cibersegurança é um tópico que está atualmente na agenda dos gestores, nomeadamente nas grandes empresas, mas que tem um impacto significativo no negócio em qualquer sector. Como clientes ou consumidores já nos confrontamos com sistemas de informação "em baixo". Enquanto profissional de cibersegurança, recordo-me por exemplo de uma transportadora aérea que tinha os aviões todos em pista porque sem sistema não conseguia identificar o que cada avião deveria transportar. Enquanto consumidor já estive num restaurante onde o menu acessível por qr-cod não estava disponível. Problemas de integridade ou confidencialidade podem causar impactos adversos similares ou maiores que problemas de disponibilidade, como mencionados. Estas áreas de atuação são o foco da prática de cibersegurança, que ajuda a identificar, gerir e reduzir os riscos. Numa altura em que o cibercrime organizado está a crescer, as empresas têm cada vez mais de investir para equilibrar a balança e continuarem a usufruir de todos os benefícios com riscos aceitáveis para as organizações, consumidores e de acordo com a legislação e regulação.

Um estudo da Deloitte de 2020 indicava que as empresas despendiam entre 4% e 10% do seu *budget* de IT em cibersegurança, mas certamente que hoje os valores serão superiores. É preciso ter em consideração que a cibersegurança é um campo dinâmico, e as ameaças estão em constante evolução, logo é importante ter presente que as empresas devem adotar uma abordagem adaptativa e contínua para alocar recursos, ajustando os investimentos conforme a dinâmica no cenário de ameaças e no contexto de negócio. Os típicos investimentos variam também por sector de atividade, dependência e grau de risco e também considerando o tamanho das organizações. A crescente utilização da tecnologia, bem como o aumento da exigência regulatória irá continuar a exigir cada vez mais investimentos, para que as empresas possam continuar a tirar partido da eficiência e eficácia resultante da tecnologia.

DERYCK MITCHELSON
Chief Information Security Officer e C-Suite Advisor da Check Point Software

A digitalização, e a sua posterior aceleração, trouxeram novos desafios para as empresas. Atualmente, para se protegerem bem como aos seus clientes, precisam de investir e ter muitos mais cuidados no que toca às superfícies de ataque que uma solução de cibersegurança tem de proteger, sendo ainda mais crítico nas PME pela complexidade e reduzido ou inexistente número de recursos humanos especializados em segurança alocados.

Em termos percentuais, as boas práticas de alocação orçamental para a área de cibersegurança indicam que se deverá investir no mínimo 10% do orçamento de TI. No entanto, este valor vai depender do sector de atividade, do nível de maturidade de cibersegurança da empresa. Uma alocação na ordem de 10% do orçamento para a área de cibersegurança é um valor aceitável, correto e confortável. Esta percentagem deve ser dividida em vários níveis de investimento. Para assegurar bons resultados na área de cibersegurança, é preciso começar por formar as pessoas, apostar em soluções de infraestrutura e *software*, que tenham como foco serem soluções compreensivas, consolidadas e colaborativas que levem os responsáveis de segurança (CISO) a criar uma política robusta de segurança de informação e ter uma ferramenta de gestão do ecossistema organizacional e de reporte de incidentes integrada.

No entanto, nunca estamos 100% seguros. Logo a seguir a ser conhecida e controlada uma ameaça, aparece uma nova. Todos os dias os especialistas se deparam com novos processos de ataque que têm de analisar e controlar. Para debelar ou evitar este tipo de eventos, é responsabilidade de cada CISO ter uma visão preventiva de segurança, onde monitorizar, validar, testar todos os vetores e superfícies de ataque passa a ser uma postura e atividade diária pro-ativa, reduzindo drasticamente o sucesso de um potencial ataque.

JOÃO SEQUEIRA
Director for the Secure e-Solutions da GMV em Portugal

Vivemos num mundo cada vez mais digital, onde a cibersegurança é uma peça fundamental na gestão do risco de qualquer organização. Com o aumentar das ameaças cibernéticas como roubo de dados *ransomware*, e outros ataques à infraestrutura digital de uma empresa, leva-nos a pensar que tem de haver investimento para salvaguardar a informação bem como a reputação de uma empresa.

Quando pensamos no investimento em cibersegurança um ponto fulcral é que prevenir é sempre significativamente mais barato.

Como em qualquer área, para chegarmos a um valor a ser distribuído este deve ter um claro Return on Investment mas quando falamos da cibersegurança o valor pode não ser óbvio. Como o cenário das ameaças é dinâmico quando se acumula uma quantidade relevante de dados, já há um novo modelo de ameaça para o qual não temos dados. Para calcular quanto deve ser atribuído à cibersegurança em primeiro lugar é necessário fazer uma correta análise de risco, bem como normas e *standards* que devem ser cumpridos. Sabemos que uma empresa na área financeira ou de saúde terá um maior investimento na cibersegurança, mas empresas mais pequenas também não devem descurar o tema, devendo pelo menos ter um sistema de gestão da segurança da informação, antivirus, *firewall*. Um outro ponto relevante prende-se com a postura de segurança de uma empresa, manter um sistema existente é menos oneroso que criar um novo. Segundo a Gartner, uma empresa deve alocar aproximadamente 5% do seu orçamento de IT à cibersegurança. Este número não se adequa a todas as empresas, e sectores mais sensíveis como a banca, alocam em média 10% do orçamento.

Quando estamos a considerar o orçamento para a cibersegurança numa empresa não existe uma abordagem única. Este deve ser justificado com base nos riscos a que estamos expostos, requisitos legais, a postura da empresa e os seus objetivos. O investimento em cibersegurança não é apenas uma decisão financeira, mas um aspeto crucial na proteção da reputação da empresa e confiança dos clientes.

BRUNO CASTRO
CEO
da VisionWare

Os ciberataques são dos principais desafios que as empresas e organizações enfrentam de forma diária. Não há uma resposta única para determinar a percentagem ideal de orçamento a ser dedicada à cibersegurança, já que cada empresa tem suas particularidades e necessidades específicas.
Contudo, de uma forma genérica, especialistas recomendam que as empresas dediquem 10-12% do orçamento à cibersegurança. Essa faixa poderá variar dependendo da dimensão da empresa, sector de atuação, nível de sensibilidade das informações geridas e complexidade da infraestrutura.
A cibersegurança deverá constituir uma rubrica indispensável de investimento dos sistemas de informação das organizações. O investimento implicado deverá estar diretamente relacionado com o risco de ciberataque ligado ao impacto dos sistemas de informação dentro da organização; por exemplo, um banco deverá gastar uma % superior do seu orçamento (relativamente a outros sectores), uma vez que terá muito mais a perder com um eventual incidente informático, como a perda total da confiança dos seus clientes. Desta feita, o cálculo da % deverá estar intrinsecamente associado ao controlo do risco de operações, devendo alocar o orçamento para gastos em cibersegurança baseado numa análise de risco, mantendo os níveis de segurança suficientes para contrapor qualquer risco ou impacto negativo ao negócio, ou até mesmo, para evitar a total perda de atividade.
Será vital olhar para o investimento em segurança não como um gasto, mas antes como um investimento regular e contínuo para fazer face a eventuais quebras de atividade e danos negativos. É essencial proteger os ativos das empresas, valorizá-los, minimizando quaisquer impactos nocivos às empresas.
Com base na experiência, recomendamos que seja efetuada uma análise baseada no risco que determinará uma % do investimento alocado à atividade em cibersegurança, a qual deverá rondar valores reais, acreditamos, situados entre os 20-30%.
A cibersegurança não deve ser vista apenas como um custo adicional para as empresas, mas como um investimento que trará retorno a longo prazo. Um ataque cibernético poderá causar danos irreparáveis à reputação de uma empresa, além de prejuízos financeiros avultados, perda de confiança e de clientes. Por outro lado, investir em cibersegurança poderá aumentar a confiança dos clientes e parceiros de negócios, além de reduzir os riscos de interrupções no funcionamento dos sistemas e perda ou fuga de dados.

MARIA ANTÓNIA SALDANHA
Country Manager
da Mastercard Portugal

A cibersegurança existe para fortalecer componentes vulneráveis de determinadas empresas contra eventuais incidentes e é esse o nosso primeiro objetivo. Contudo, quando se dimensiona o investimento em cibersegurança, deve, também, ter-se em consideração uma visão holística de todas as entidades que se relacionam num determinado ecossistema para se conseguir aumentar substancialmente a ciber resiliência.
Isto é, se considerarmos que o cibercrime custa à economia global cerca de 5% do PIB mundial (cerca de 5 triliões de euros) e que o conjunto de inter-relações que as empresas têm entre si, então, facilmente nos apercebemos que os desafios da cibersegurança ultrapassam aquilo que ainda há uns anos considerávamos os limites naturais das organizações.
E se em cima disto pusermos os desafios associados à engenharia social, ao teletrabalho ou ao e-commerce, então os requisitos para a cibersegurança ganham uma dimensão ainda mais relevante.
Esta a abordagem a um "nós" coletivo em cibersegurança cruza uma linha, por vezes, invisível, que separa uma empresa dos seus parceiros, e é uma abordagem desafiante se tivermos em consideração que apenas 53% das empresas afirmam confiar plenamente na segurança cibernética dos seus parceiros .
Por outro lado, avaliar os problemas de segurança dos parceiros pode não ser uma tarefa fácil e as autoavaliações correm o risco de não serem credíveis se não forem validadas por uma entidade independente. Neste caso, o problema não é tanto a natureza paternalista de muitas abordagens, mas as dúvidas que levanta acerca da eventual pouca confiabilidade da empresa parceira.
Além disso, muitas empresas, principalmente as de menor dimensão, enfrentam, por vezes, o dilema sobre o tipo de investimento que devem fazer para se manterem competitivas. Isto é, se devem investir em tecnologia produtiva ou se devem investir em cibersegurança .
Diferentes indústrias enfrentam, também, diferentes desafios e, por isso, a decisão sobre a dimensão do orçamento em cibersegurança deve ser o resultado de uma equação que ponha em proporção o ganho obtido pelas reduções marginais no risco em relação aos investimentos necessários e, portanto, tudo se resume a um equilíbrio entre as duas escolhas.

Inteligência de ameaças é a melhor defesa na antecipação de ciberataques

Uma estratégia de segurança inteligente deve ser capaz de prevenir eficazmente as ameaças e responder aos incidentes de uma forma abrangente. Uma reação rápida, centralizada e controlada é essencial para uma gestão eficaz dos incidentes e a única forma de estar um passo à frente das ameaças.

Nos últimos anos, múltiplos relatórios e relatos de ciberataques pintaram um quadro que mostra bem como os atacantes desenvolveram as suas capacidades e se passaram a organizar em redes profissionais. As tentativas de ataque multiplicam-se e a sofisticação das violações de segurança cresceu exponencialmente. Com melhor financiamento, os cibercriminosos melhoraram as suas táticas, técnicas e procedimentos. Além disso, as abordagens tornaram-se mais difíceis de detetar e menos previsíveis. Caracterizam-se pela furtividade e persistência, de modo a ter tempo para fazerem movimentos laterais e infetar os sistemas informáticos das suas vítimas em profundidade, tornando impossível a reversibilidade.
Neste cenário incerto e em constante mudança, o papel das equipas de segurança tornou-se muito mais complicado. De facto, a complexidade nos ambientes informáticos tornou-se num dos maiores desafios, especialmente para as pequenas e médias empresas em todo o mundo.

O aliado dos profissionais de segurança
Por conseguinte, é essencial que as empresas de cibersegurança atualizem as suas soluções para conseguirem proporcionar a proteção de que as empresas realmente precisam, permitindo-lhes recorrer à inteligência de ameaças para construir uma linha proactiva de defesa que permita proteger os ativos digitais da empresa contra uma variedade de ameaças.
A sua eficácia provém de uma combinação de tecnologias inteligentes e da perícia das equipas de segurança. Deve proporcionar os alertas relevantes para que estes especialistas possam conduzir as suas investigações com rapidez e precisão, porque o tempo é essencial se o ataque for confirmado. Neste contexto limitado, a eficácia da análise da informação é um fator determinante para uma avaliação de risco relevante.
Esta segurança inteligente baseia-se em três pilares que se devem complementar: a capacidade de utilizar enormes quantidades de dados para detetar as mais pequenas pistas, o fator humano e a proposta de inteligência de ameaça, e a sua capacidade de responder às necessidades dos clientes.
O panorama de ameaças dos dias de hoje está em rápida evolução e muitas organizações enfrentam ameaças complexas e persistentes. A inteligência de ameaças tornou-se, assim, parte integrante do conjunto de ferramentas imperativo de uma equipa de segurança.
Além disso, a inteligência de ameaças é uma estratégia proactiva, uma vez que melhora a eficiência e o tempo de resposta e instila uma mensagem dissuasiva aos atacantes: uma abordagem proactiva à segurança cibernética e a garantia de uma resposta rápida e eficaz por parte de equipas experientes de "resposta rápida".

Por que é a inteligência de ameaças tão importante?

A inteligência de ameaças é uma parte crucial de qualquer ecossistema de segurança cibernética. Um programa de inteligência de ciberameaças, também por vezes designado de CTI, pode:

Evitar perda de dados: com um programa de CTI bem-estruturado, as organizações podem identificar ameaças cibernéticas e impedir que violações de dados libertem informações confidenciais.

Indicar as melhores medidas de segurança: ao identificar e analisar ameaças, o CTI identifica padrões que os atacantes usam e ajuda as organizações a implementarem medidas de segurança para se protegerem contra futuros ataques.

Informar outras pessoas: os cibercriminosos estão cada vez mais inteligentes. Para os acompanhar, os especialistas em cibersegurança partilham as táticas observadas na sua comunidade para criar uma base de conhecimentos coletiva e combater o cibercrime.

Especial Cibersegurança

PAULA FERNANDES
Security Business Group Lead na Microsoft Portugal

Nos últimos anos, registou-se um aumento significativo do número e da sofisticação dos ataques cibernéticos. Só em 2022, a Microsoft analisou 70 biliões de sinais e bloqueou 65 mil milhões de ataques. A cibersegurança é um trabalho permanente e o nosso compromisso passa por recorrer a dados e inteligência para continuar a evoluir a capacidade de prevenção, resposta e mitigação de riscos, à medida que navegamos o mundo crescentemente híbrido e multi-cloud. Ajudamos as empresas no processo contínuo, mas os valores a alocar dependerão da atividade, necessidades específicas, e do potencial de risco de cada empresa. Ainda assim, há dados que nos podem ajudar a ter uma perceção das tendências de investimento. A Gartner estima que os gastos globais em segurança e gestão de risco cresçam mais de 11% ao longo deste ano e é expectável que esse número duplique até 2026. Segundo o *survey* divulgado no último Gartner IT Symposium, 66% dos CIOs admitem aumentar o investimento em cibersegurança. Em resumo, a cibersegurança tem de ser uma prioridade das organizações e essa alocação deve ser medida tendo em consideração o grau de maturidade e postura de segurança presente e o potencial nefasto de um eventual (quase inevitável) *breach*.
Porque sabemos que as empresas têm de equilibrar os seus investimentos, procurando ser cada vez mais eficientes e produtivas, anunciámos o Microsoft Security Copilot, uma solução única no mercado que combina grandes modelos de linguagem da OpenAI com o nosso modelo de segurança, alimentado por uma vasta inteligência de todos os sinais que recebemos e bloqueamos diariamente. Este é o primeiro produto de segurança com IA generativa, e que poderá simplificar o trabalho das equipas de segurança das organizações, amplificando as capacidades dos profissionais. Este serviço faz a identificação de atividades maliciosas, ajuda a correlacionar e resumir dados dos ataques, disponibiliza recomendações para ações de mitigação e faz prevenção de ameaças em tempo real, além de aprender com a informação gerada.
A cibersegurança é um imperativo para todas as organizações e as suas consequências podem ser dramáticas, em particular, para PME, que compõem 99% do tecido empresarial português. Segundo o Instituto Ponemon, podem custar entre 33 mil e 500 mil euros, e representar unidades de investimento bastante inferiores aos custos que terão na sequência de um ataque.

JOSÉ GONÇALVES
Cybersecurity Specialist da Exclusive Networks

É importante notar que, embora investir em cibersegurança possa ser caro, o custo de uma violação ou incidente pode ser muito maior, incluindo perdas financeiras, danos à reputação (de difícil cálculo das reais perdas financeiras), responsabilidades legais e multas regulatórias. Por conseguinte, é essencial encontrar um equilíbrio entre o custo das medidas a implementar e os potenciais riscos e custos associados a uma violação.
Como regra geral, uma empresa deve alocar cerca de 5-10% do seu orçamento de TI para a cibersegurança, dependendo do tamanho e complexidade de sua infraestrutura de TI e do nível de risco que enfrenta. No entanto, este montante pode variar muito, e as empresas devem consultar especialistas em cibersegurança para determinar o nível de investimento adequado às suas necessidades e requisitos específicos.
Para garantir que o orçamento alocado para cibersegurança é suficiente, uma empresa deve tomar as seguintes medidas: realizar uma avaliação de risco (primeiro passo é avaliar os riscos de cibersegurança enfrentados. Isso ajudará a determinar a probabilidade e impacto potencial de uma violação ou incidente de cibersegurança); desenvolver uma estratégia de cibersegurança (com base na avaliação de risco, a empresa deve desenvolver uma estratégia de cibersegurança que delineie as medidas específicas a tomar para mitigar os riscos); omplementar controlos (uma vez desenvolvida a estratégia, a empresa deve implementar os controlos delineados); monitorizar e avaliar (a empresa deve monitorizar regularmente a eficácia dos controlos de cibersegurança implementados e avaliar a eficácia global); revisão de orçamento (empresa deve realizar uma revisão anual do orçamento para garantir que este é suficiente para cobrir os custos da estratégia de cibersegurança. Se o orçamento for considerado insuficiente, podem ser feitos ajustes para garantir a disponibilidade dos fundos necessários).

JOHN SHIER
Field CTO da Sophos

Não existe um valor mágico que garanta que, investindo em cibersegurança, as empresas não sejam vítimas de um ciberataque. O custo real vai ser diferente de uma organização para outra; o essencial é que cada uma entenda o que precisa de ser protegido e avalie criticamente a sua capacidade atual para o fazer. A lacuna entre os controlos existentes e os que falta implementar será o seu orçamento. O que posso dizer é que será sempre mais barato prevenir um ataque do que recuperar de um. Por exemplo, as cidades norte-americanas de Baltimore e Atlanta foram atingidas por *ransomware* e gastaram quase 20 milhões de dólares cada uma para recuperar deles.
Um fator a considerar é dar à equipa de cibersegurança o seu próprio orçamento, não estando este relacionado ou dependente de outras prioridades organizacionais. Uma parte do orçamento de segurança deverá ser sempre dinâmica e sujeita às prioridades do negócio. Haverá, no entanto, alguns custos recorrentes mais previsíveis a cada ano; mas mesmo estes também estão sujeitos a forças económicas. O equilíbrio entre uns e outros será parcialmente determinado pelo grau de maturidade das empresas. As organizações mais maduras terão uma base mais estável e gastarão menos tempo e dinheiro a gerir dívidas de tecnologia, a remediar a falta de proteção e a dar resposta a incidentes.

ANTÓNIO CORREIA
Area Sales Manager da WatchGuard Portugal

Não há um número mágico que se adeque a todas as empresas, sectores de atividade e dimensões. Mas a verdade é que o caminho para a transformação digital do tecido empresarial implica obrigatoriamente investimentos globais em tecnologia. Portugal é um país feito de PMEs e isso não pode ser ignorado. A nossa sobrevivência futura depende de sermos capazes de aumentar a eficiência e, para o efeito, devemos abordar os planos de digitalização urgentes de amanhã que, na sua maioria, dependem de uma gestão eficaz do PRR.
Pode dizer-se que estamos no caminho certo para entrar no comboio da inovação, que desta vez não pode ser desperdiçado, se tal acontecer Portugal sofrerá em todos os sectores e em vez de seguir em frente, volta para a casa de partida. Mas, para o fazer, há aspetos que precisam de ser eliminados o mais rapidamente possível, um deles, e o que considero o mais importante, é a abordagem ligeira que os gestores têm perante a cibersegurança. Portugal continua a ser, segundo um estudo publicado no site do Gabinete de Estratégia e Estudos do Ministério da Economia, um dos países europeus com menor volume de investimento em cibersegurança. Este cenário é preocupante quando, de acordo com o mesmo estudo, somos um dos países europeus mais vulneráveis ao cibercrime. As empresas tendem a investir mais na prevenção de falhas e menos em estratégias desenhadas para detetar e antever futuros ataques. É, por isso, essencial prevenir, detetar e responder a qualquer tipo de ciberameaças, bem como consciencializar os recursos humanos para as principais ameaças à segurança que podem afetá-los, especialmente quando estão fora do perímetro da rede da empresa, preservando a sua produtividade ao mesmo tempo. Dito tudo isto, acredito que a onda de transformação digital que está em curso no nosso país, com grande foco na importância da cibersegurança das empresas portuguesas, irá gerar oportunidades de investimento e de negócio que poderão ser fundamentais para o desenvolvimento da nossa economia.

LUCILA KOMINSKY
Chief Marketing Officer da S21sec

De um modo geral, os especialistas defendem que se deve gastar entre 10% a 15% do orçamento de IT com a proteção contra data *breaches* e ciberataques. Este é um bom parâmetro, considerando que o sector financeiro é uma das áreas mais visadas em fraudes e ataques, porém esta não é uma resposta simples e completa. Há muitos fatores que influenciam a criação de um orçamento de cibersegurança, tais como a dimensão da empresa, a indústria, o tipo de dados com que a empresa trabalha, a variedade de ativos e dispositivos, os regulamentos locais. O investimento total em cibersegurança está a aumentar de ano para ano.
De acordo com empresas como a Gartner, a previsão mundial de despesas em segurança e gestão de riscos irá crescer 11,3% em 2023 para atingir mais de 170 mil milhões de euros. Em Portugal, o investimento global em segurança irá passar de 12,5% em 2022 para 16,8% em 2023. O mercado português de cibersegurança deverá registar um CAGR de 7,7% entre 2023-2028. A vulnerabilidade e exposição a vários ciberataques aumentou, a par com o número de dispositivos IoT. Prevê-se também que o mercado registe um crescimento significativo no sector da implementação da *cloud*. A segurança tem sido crítica em cada fase do ciclo de adoção da *cloud*. À medida que o fornecimento de serviços de IT passou de uma situação interna a uma situação externa às fronteiras de uma empresa.

ANA SILVA
Territory Account Manager da Kaspersky Portugal

Um estudo da PWC afirma que o reforço da cibersegurança pelas empresas tem sido impulsionado por uma maior utilização das tecnologias digitais e um cenário de ameaça crescente. Para saber quanto as empresas estão a gastar nesta área e os seus planos para o futuro, a Kaspersky realizou 3.230 entrevistas com empresas com mais de 50 empregados em todo o mundo.
Os resultados indicam que os orçamentos em cibersegurança irão crescer globalmente nos próximos três anos cerca de 10%, quer em PMEs, quer em grandes empresas.
Entre as razões para o aumentar dos orçamentos de segurança, os inquiridos destacaram a maior complexidade das infraestruturas de TI (45,8% para PMEs e 53,7% para grandes empresas) e a necessidade de melhorar o nível dos profissionais de cibersegurança (36% para PMEs e 33,7% para grandes empresas). A incerteza geopolítica e económica é também fundamental para aumentar os orçamentos em cibersegurança (28,2% para as PME e 33% para as grandes empresas).
A continuidade das empresas depende da segurança da informação. As infraestruturas tecnológicas estão a tornar-se cada vez mais complexas e isto cria uma maior consciencialização por parte das empresas para protegerem todos os ativos corporativos. A regulamentação em cada país é também um fator de aumento dos orçamentos de cibersegurança, à medida que os mercados regulamentares se tornam mais apertados, tanto em setores especializados como no geral.
Para aumentar a eficácia dos investimentos em segurança cibernética e reduzir o risco de ataques e violações de segurança, o endpoint deve ser protegido com soluções que incluam capacidades de deteção de ameaças e de resposta, estratégia esta reforçada com formação específica em cibersegurança para funcionários.

ALAIN SANCHEZ
EMEA Field CISO da Fortinet

Quando se quantifica o investimento num determinado domínio como uma fração das receitas da empresa, torna-se uma preocupação da administração. Como a cibersegurança tem a missão de tornar o nosso mundo mais seguro, é legítimo que a comissão executiva faça uma avaliação comparativa dos seus custos da cibersegurança. Como

nenhuma empresa está imune à ameaça, a cibersegurança torna-se cada vez mais escrutinada pelos *stakeholders*. Estarão os principais ativos da nossa cadeia de valor bem protegidos? Será que dimensionamos devidamente as nossas defesas contra uma ameaça cada dez mais sofisticada? Como é que o contexto geopolítico aumenta a ameaça? As nossas ferramentas de cibersegurança são suficientemente sofisticadas para garantir resistência?
Estas são boas questões. Em parte, porque estarão na mente de todos os *stakeholders* quando ocorrer o ataque, e também porque o ciber risco precisa de ser aprovisionado financeiramente. Neste sentido, a forma mais direta é perguntar a empresas tradicionalmente bem equipadas a importância da cibersegurança como uma fração dos seus gastos em TI. Em média, as organizações gastam 10% dos seus orçamentos de TI em cibersegurança, segundo o relatório IANS & Artico, Security Budget Benchmark Summary de 2022.
Mas estas também são perguntas enganadoras. A cibersegurança evolui rapidamente de um centro de custos para um inspirador de transformações digitais ambiciosas. Assim, em vez de a reportar como uma fração do resultado, a nova geração de Cyber Security Officers relaciona-a com o desempenho incremental da empresa possibilitado pela cibersegurança. Em domínios críticos como a triagem de eventos, por exemplo, quando se trata de incidentes de segurança e gestão de eventos em que os operadores especializados precisariam de 20 minutos para classificar um ataque real a partir de um conjunto de falsos positivos, a FortiSOAR demora três minutos. A submissão de um ficheiro ao motor de detonação da *sandbox* demora cerca de um minuto, em que o tempo de avanço manual varia de uma a seis horas. Corrigir e responder a um incidente é conseguido em cerca de cinco minutos pela integração do Security Fabric, em vez de uma hora. No total, o tempo de espera das oito operações que constituem a maior parte da atividade de um Centro de Operações de Segurança passa de 15 horas para cerca de 20 minutos.
Isto explica porque estamos a entrar tão fortemente na era das plataformas integradas e a abandonar a abordagem da velha guarda. Basta aplicar o tempo poupado numa tabela ao rendimento por hora alcançado pelas empresas para desenvolver um argumento comercial indiscutível para o seu próximo investimento em cibersegurança. É muito mais provável ganhar a atenção da direção desta forma do que as abordagens excessivamente utilizadas e orientadas para os custos.

NABIL DIAB
Head of Cibersecurity da Alter Solutions

Há uma questão primária essencial, à qual devemos responder primeiro: que orçamento deve uma organização atribuir às TI? Apenas com essa informação conseguimos compreender o investimento necessário para a cibersegurança.
Na Alter Solutions acreditamos que o orçamento das TI é um ponto crucial quando falamos de orçamento de cibersegurança, porque a primeira camada da cibersegurança é a higiene das TI. Com isto queremos dizer que o Departamento de TI deve ter ferramentas e colaboradores de TI com competências, experiência e tempo suficientes para gerir, manter e melhorar corretamente o sistema de organização da informação.
Comparando com o exemplo da saúde de uma pessoa: não é por ter um grande orçamento para médicos que alguém estará necessariamente em boa forma, mas sobretudo, por adotar um estilo de vida saudável (dieta, stress, desporto, etc.). O mesmo se aplica à segurança informática: se a empresa tiver uma má higiene informática, pode gastar milhões de Euros nos melhores produtos de cibersegurança do mercado, que continuará a ser altamente vulnerável.
Quanto ao orçamento de TI a atribuir, este varia consoante a tipologia da empresa: quanto mais as TI estiverem no coração do negócio, mais elevado deverá ser o seu orçamento. Podemos analisar dois extremos (excluindo fornecedores de serviços de TI, como a Alter Solutions): bancos e hospitais.
Atualmente, os bancos são extremamente dependentes dos serviços de TI devido à digitalização (quase) total do negócio. Os seus milhares de operações críticas diárias dependem dos serviços de TI. Assim, a dotação orçamental para TI cresceu e pode atingir até 25% do orçamento global.
Os hospitais estão a mudar para um mundo digital, desde a digitalização dos registos dos doentes até à ligação dos dispositivos médicos. Apesar de estas operações estarem relacionadas com vidas humanas, a área de TI é menos prioritária em comparação com outros componentes, quando o orçamento para dispositivos e funcionários é atribuído, e pode ser demasiado baixo.
Assim, na Alter Solutions consideramos que o orçamento de TI deve ser entre 4% e 25% dos custos globais e, quando este se encontra definido de forma adequada, é possível atribuir um orçamento dedicado à cibersegurança na ordem dos 10 a 15% do orçamento de TI.

CARLA ZIBREIRA
Digital Trust Business Unit Manager na Axians

O atual e evolutivo ecossistema de ciberameaças manterá a pressão sobre as organizações para que ampliem e aprofundem as estratégias de defesa cibernética, expandindo a capacidade de deteção e melhorando a resposta a incidentes. Como tal, investir em cibersegurança deixou de ser opcional para passar a ser parte integrante do plano estratégico e de investimentos de qualquer organização.
Dados dos últimos anos mostram que as organizações investem cada vez mais em cibersegurança. A Gartner prevê que os gastos globais com segurança e gestão de riscos crescerão mais de 11% em 2023, de 158 mil milhões dólares em 2021 para 188 mil milhões. Espera-se que a tendência continue uma subida na ordem dos 11% até 2026, atingindo um total de 267,3 mil milhões. De acordo com dados recolhidos pela Statista, as organizações alocam pelo menos 12% de seu orçamento de TI em segurança da informação. A maior contribuição foi realizada em 2020, com 12,8%. Até 2022, as empresas alocaram 12,7% do seu orçamento para segurança de TI. Ainda assim, o número de ataques tem vindo a crescer, assim como o custo que atingiu um recorde histórico em 2022, com o custo médio de uma violação de dados estimado em 4,35 milhões, representando 2,6% de aumento em relação ao ano de 2021 (IBM Cost of a Data Breach Report 2022).
"Mas afinal, qual é o investimento necessário para se estar seguro?". Infelizmente a resposta não é direta e seria mais fácil se houvesse um número ou uma fórmula universal ditando quanto se deveria alocar orçamentalmente à segurança cibernética, mas depende muito. Depende muito de vários fatores mas sobretudo de uma abordagem sustentada na gestão de risco e o consequente equilíbrio entre a exposição ao risco e o custo de um potencial incidente de cibersegurança. A definição do orçamento de segurança deve ser um processo proativo, que entenda o propósito da organização e ainda as motivações, riscos e oportunidades do ecossistema do ciberespaço. Que equacione aspetos como a dimensão do negócio, potencial de crescimento do negócio, complexidade e *status* do ecossistema tecnológico, o nível de maturidade relativamente à cibersegurança, assim como a valorização do risco de cibersegurança.
Mais gastos com cibersegurança não significa mais cibersegurança! É fundamental que os orçamentos sejam exercícios sustentados no conhecimento efetivo dos riscos, que permaneçam na linha de frente de qualquer estratégia de negócio na dimensão e na certeza de que o seu contributo para a resiliência do negócio se traduza na saúde financeira do mesmo.