VIEIRA DE ALMEIDA

CYBERSECURITY SERIES I

fevereiro 2022

CYBERSECURITY SERIES I

CIBERSEGURANÇA – AMEAÇAS, DESAFIOS E AÇÕES PARA 2022

fevereiro 2022

A cibersegurança é um tópico cada vez mais relevante devido ao aumento contínuo dos ciberataques: a transição para a economia digital, juntamente com os impactos da pandemia da COVID-19, estão a potenciar o crescimento das ciber ameaças.

Os últimos dois anos foram fortemente marcados pela ocorrência de ciberataques de grande dimensão, tendo os ataques de *malware* emergido como a ameaça mais relevante na UE e o *phishing*, o roubo de identidade e o *ransomware* aumentado de forma substancial.

O Relatório Global de Risco do Fórum Económico Mundial para 2022 destaca exatamente a cibersegurança como um risco crescente para as indústrias e organizações. Não constitui, por isso, qualquer surpresa que a cibersegurança esteja a ser objeto da atenção crescente dos legisladores e reguladores nacionais e europeus.

As **Cybersecurity Series** analisam os temas legais e regulatórios de cibersegurança que as organizações devem ter em conta e para os quais se devem preparar. Esta primeira edição estabelece o mote para o que é um aspeto inevitável (e indispensável) da estratégia de cibersegurança de uma organização.

Ireland's Department of Health and Health Service Executive
O ataque forçou o *shutdown* dos seus sistemas e culminou na interrupção de procedimentos médicos digitais, tais como serviços de diagnóstico

CNA Financial e Gallagher
Ambas as seguradoras sofreram um ataque de *ransomware* que comprometeu as suas redes, incluindo os dispositivos de trabalho remoto

Magellan Health
Um ataque de *ransomware* comprometeu os dados de aproximadamente 365 000 doentes

Twitch
Ataque resultou no *leak* de mais de 125GB de dados, incluindo código fonte da empresa, salários e dados pessoais de utilizadores

Impresa
A empresa de *media* sofreu um ciberataque que se traduziu no roubo de dados pessoais de clientes e na interrupção das suas operações e serviços

Colonial Pipeline
Ataque de *ransomware* incidiu sobre mais de 100GB de dados e pôs em risco as operações da empresa, iniciando uma crise energética local durante vários dias

Sistema bancário grego
Após o *hacking* de um website de viagens grego, os quatro principais bancos da Grécia cancelaram e substituíram aproximadamente 15 000 cartões de crédito e débito de clientes

EasyJet
Ataque resultou no acesso ilegítimo a dados de 9 milhões de clientes, incluindo registos de cartões de crédito

Microsoft
Ataque a servidores da Microsoft Exchange terá afetado mais de 60 000 vítimas, incluindo empresas e entidades governamentais

OS DESAFIOS

MAIS DIGITALIZAÇÃO, AUTOMAÇÃO E CONECTIVIDADE IMPULSIONADAS PELA COVID-19 E 5G/IOT

As alterações nos padrões de trabalho impulsionadas pela COVID-19 aumentaram substancialmente as vulnerabilidades de cibersegurança: múltiplos pontos de acesso, áreas de exposição maiores e a larga utilização de redes domésticas (tipicamente mais desprotegidas) tornaram-se um alvo central para ciberataques. **52%** dos líderes em matéria legal e de *compliance* estão preocupados com os riscos de cibersegurança resultantes do trabalho remoto. Adicionalmente, os dispositivos IoT, potenciados pelo 5G, são particularmente vulneráveis a ciberataques, estando previsto que o número global de dispositivos conectados atingirá **41.6 mil milhões em 2025**. A utilização generalizada de IA, *machine learning* e serviços de computação em nuvem trazem também novos riscos de cibersegurança.

AUMENTO DOS ATAQUES DIRIGIDOS A SECTORES ESPECÍFICOS

Certos sectores são mais suscetíveis aos riscos de cibersegurança, tais como os que utilizam dados sensíveis ou valiosos. É o caso, por exemplo, do sector da saúde (os incidentes no sector da saúde aumentaram **58%** em 2020), do sector bancário e financeiro (tendo em conta a crescente digitalização do sector através dos serviços de pagamento, moeda eletrónica e cripto-ativos) e do comércio eletrónico (com fraudes de cartão de crédito e a utilização fraudulenta de credenciais de identificação).

PROLIFERAÇÃO DE CERTOS TIPOS DE ATAQUES

Antecipa-se que os ataques de *phishing*, *ransomware*, DDoS, abuso de credenciais de acesso privilegiado e ataques de segurança *endpoint* aumentem. Adicionalmente, os ataques a dispositivos IoT e executados através de dispositivos móveis estão a tornar-se cada vez mais frequentes, o mesmo sucedendo com ataques e espionagem patrocinados pelos Estados.

MAIOR DEPENDÊNCIA DE TERCEIROS

A segurança das cadeias de valor/fornecimento está a tornar-se cada vez mais relevante dado que as empresas dependem crescentemente de terceiros, incluindo prestadores de serviços de segurança e seguradoras, no exercício da sua atividade. A implementação de medidas para garantir a segurança das cadeias de valor está a tornar-se uma obrigação legal.

FALTA DE *EXPERTISE* EM CIBERSEGURANÇA

A implementação de políticas internas de cibersegurança, de quadros de resposta a incidentes e a formação de funcionários são cada vez mais relevantes para garantir a resiliência contra ciberataques. Com efeito, 95% dos incidentes são motivadas por erro humano e 30% das "fugas de dados" envolvem colaboradores internos.

AUMENTO DA COMPLEXIDADE DOS DESAFIOS DE CIBERSEGURANÇA

Os instrumentos, técnicas e procedimentos utilizados para executar ciberataques são cada vez mais sofisticados e direcionados (bem como adaptados) a empresas de grande dimensão. Simultaneamente, CaaS (*cybercrime-as-a-service*) e RaaS (*ransomware-as-a-service*) estão em crescimento, com os atacantes cada vez mais dispersos e recorrendo a tecnologias emergentes tais como ambientes *multi-cloud* e tecnologias 5G.

AS TENDÊNCIAS

AUMENTO DOS ORÇAMENTOS PARA A CIBERSEGURANÇA

Tanto as organizações públicas como as privadas investem cada vez mais em cibersegurança, sendo reconhecido que esta é um fator de sucesso bem como uma condição para que uma empresa ou marca seja de confiança. Os gastos mundiais alocados à cibersegurança atingirão $174,7 mil milhões (USD) em 2024.

AUMENTO DAS DESPESAS EM SECTORES ESPECÍFICOS

O aumento das despesas com a cibersegurança será particularmente visível nos sectores da saúde, bancário e financeiro, seguros, tecnologia, telecomunicações, *medi*a e os sectores público e social. Não obstante, e tendo em conta a legislação e obrigações regulatórias futuras, como seja na UE, espera-se que também outros sectores atribuam uma porção cada vez mais significativa do seu orçamento à cibersegurança.

NOVAS FERRAMENTAS TECNOLÓGICAS PARA A CIBERSEGURANÇA – DESIGNADAMENTE IA E AUTOMAÇÃO

As ferramentas utilizadas no combate às ciber ameaças têm um nível de sofisticação cada vez maior. Prevê-se que a autenticação sem palavras-passe e as aplicações de segurança e controlo em ambientes *cloud*, tais como as CASB (*Cloud Access Security Broker*) e as CWPP (*Cloud Workload Protection Platforms)*, estarão entre as tecnologias de segurança mais influentes no futuro. A IA tornar-se-á também uma tecnologia central, sendo que esta e tecnologias como *machine learning* permitirão o autodiagnóstico e a autoproteção autónomas dos dispositivos, podendo também ser utilizadas para avaliar o comportamento dos utilizadores e detetar sinais de ciberataques através da correlação de eventos.

DESENVOLVIMENTO DE *KNOW-HOW*

A formação de colaboradores em matéria de cibersegurança, bem como a realização de simulações de ataques e incidentes, terão um papel cada vez mais relevante, sendo essencial a cooperação de todos os *stakeholders* ao longo da cadeia de valor para enfrentar a multiplicidade de desafios de cibersegurança.

DESENVOLVIMENTO DE PARCERIAS PÚBLICO-PRIVADAS PARA COMBATER AMEAÇAS

A cooperação público-privada desempenhará um papel cada vez mais significativo na abordagem aos desafios de cibersegurança, incluindo através da partilha de dados e conhecimentos especializados, na definição de políticas públicas, em ações de capacitação, bem como em certificações e normas de cibersegurança.

CRESCIMENTO DA INDÚSTRIA DA CIBERSEGURANÇA

Antevê-se que o mercado global de cibersegurança cresça de 167,1 mil milhões de dólares em 2019 para 248,26 mil milhões de dólares em 2023. Os serviços de cibersegurança serão o maior e mais rápido segmento de crescimento do mercado de segurança, seguido pelo *software*.

AUMENTO DOS REQUISITOS REGULATÓRIOS E SANÇÕES RESULTANTES DE INCIDENTES DE CIBERSEGURANÇA

Está prevista a aprovação de novas regras de cibersegurança na UE, tais como a Proposta de Diretiva relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na UE (NIS II), bem como a Diretiva relativa à resiliência das entidades críticas (CER). No sector financeiro, a proposta de Regulamento relativo à resiliência operacional digital do sector financeiro (DORA) irá acarretar novas obrigações mais exigentes. A nível nacional, foi aprovado o Decreto-Lei n.º 65/2021 que Regulamenta o Regime Jurídico da Segurança do Ciberespaço e define as obrigações em matéria de certificação da cibersegurança. Adicionalmente, muitos sectores têm as suas próprias disposições específicas em matéria de cibersegurança, com o RGPD a abordar especificamente as violações de dados pessoais. A complexidade das regras legais com impacto na cibersegurança e as respetivas coimas estão a aumentar, exigindo uma atenção acrescida por todos os *stakeholders*.

As organizações devem desenvolver e implementar proativamente uma **estratégia de cibersegurança** sob os princípios da prevenção, reação e monitorização. A implementação desta estratégia requer necessariamente uma abordagem e análise holísticas, de modo a identificar e melhor abordar os riscos legais, operacionais, financeiros e de reputação.

AÇÕES PARA 2022

AVALIAÇÃO DE CIBERSEGURANÇA

Mapear os processos e documentação da sua organização e avaliar o seu nível de resiliência de cibersegurança, incluindo em relação a fornecedores, parceiros, trabalhadores e clientes.

RESILIÊNCIA DE CIBERSEGURANÇA

Elaborar políticas internas de cibersegurança, implementar medidas técnicas e organizacionais, cumprir as certificações exigidas e as normas aplicáveis, realizar auditorias e subscrever seguros.

RESPOSTA A INCIDENTES DE CIBERSEGURANÇA

Identificar e registar incidentes de cibersegurança, recolher provas, realizar análises de risco, implementar ações de contenção e recuperação, enviar todas as comunicações e notificações necessárias às partes e autoridades reguladoras relevantes, bem como conceber e implementar uma estratégia de mitigação de acordo com os riscos identificados.

SENSIBILIZAÇÃO E CAPACITAÇÃO

Realizar ações regulares de formação de funcionários e implementar programas internos que aumentem a atenção e vigilância a temas de cibersegurança. Estabelecer programas de cooperação para capacitação com parceiros comerciais e prestadores de serviços.

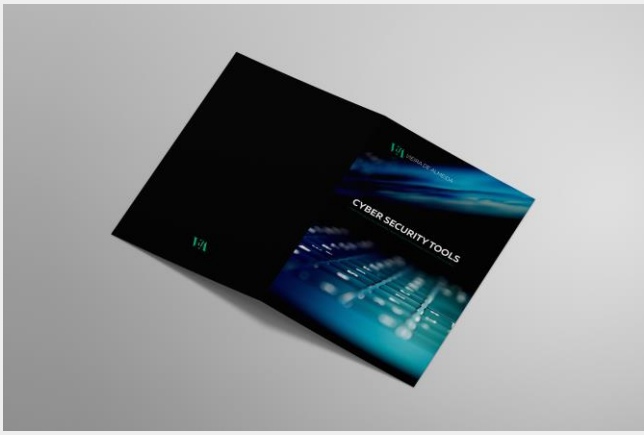
MONITORIZAÇÃO CONTÍNUA

A cibersegurança é um processo contínuo. Deve garantir que a sua estratégia de cibersegurança está em conformidade com as dinâmicas de mercado e atualizações regulatórias.

VdA CYBERSECURITY TOOLS

A VdA desenvolveu as **Cybersecurity Tools** para ajudar as organizações a lidar com a crescente complexidade legal e regulatória da cibersegurança.

Integrando três programas (*Cyber Resilience Programme*, *Cyber Incident Response Programme* e *Cyber Focused Business Programme*), as Cybersecurity Tools asseguram que a sua organização está inteiramente preparada para responder aos desafios de cibersegurança através de uma abordagem holística que tem em consideração as particularidades da organização e do respetivo sector.



www.vda.pt

MAGDA COCCO
Sócia Responsável da área
mpc@vda.pt

INÊS ANTAS DE BARROS
Sócia
iab@vda.pt

MARIA DE LURDES GONÇALVES
Associada Coordenadora
mlg@vda.pt

HELENA CORREIA MENDONÇA
Consultora Principal
hcm@vda.pt