



OVERVIEW 2021

TOP VULNERABILIDADES E RECOMENDAÇÕES

MAIO 2022



PORTUGAL

Edifício Atrium Saldanha
Praça Duque de Saldanha, n° 1,
2º andar
1050-094, Lisboa | Portugal
T: +351 21 33 03 740
E: info@integrity.pt

UNITED KINGDOM

43 Berkeley Square
Mayfair, Westminster
London, W1J 5FJ | U.K.

ESPAÑA

Calle Cronos 63, 4ª planta
Oficina 2
28037, Madrid | España
T: +34 91 376 88 20

ÍNDICE

SOBRE A INTEGRITY	3
QUEM SOMOS?	3
INTRODUÇÃO	4
TOP VULNERABILIDADES E RECOMENDAÇÕES	4
PENTESTING	6
KEEP-IT-SECURE-24	8
OVERVIEW	8
PROCESSO DE TESTES	11
PENTESTING OVERVIEW 2021	12
ENQUADRAMENTO DAS MÉTRICAS	12
Entidades	12
Sobre os assets	13
Tendências	14
VULNERABILIDADES	16
Severidade das vulnerabilidades	16
Top 5 tipos de vulnerabilidades	21
CICLO DE VIDA DAS VULNERABILIDADES	43
TEMPOS DE VIDA	49
TEMPO DE VIDA PARA AS 5 VULNERABILIDADES MAIS RESOLVIDAS EM 2021	49
CONCLUSÃO	53
TOP VULNERABILIDADES E RECOMENDAÇÕES	53



SOBRE A INTEGRITY QUEM SOMOS?

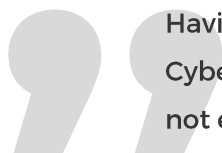
A **INTEGRITY** é uma empresa portuguesa de Consultoria e Auditoria Tecnológica com enfoque na área da Cibersegurança, que presta um serviço especializado e inovador aos seus clientes, garantindo a proteção e segurança do seu ativo mais precioso - a informação - contra potenciais incidentes e prejuízos.

Desde junho de 2021 que a INTEGRITY faz parte do Grupo Devoteam, o que lhe permitiu expandir a sua oferta a um número maior de geografias, clientes e atividades, mantendo os co-fundadores da INTEGRITY a sua gestão.

Certificada pela ISO 27001 (Segurança da Informação) e ISO 9001 (Qualidade), pelo PCI e membro CREST e do CIS - Center for Internet Security, a INTEGRITY cumpre, desde sempre, com os critérios mais rigorosos de qualidade, confidencialidade, integridade e segurança, assumindo todos os colaboradores este compromisso.

Com 13 anos de experiência e a operar em 19 países nos 5 continentes, a empresa oferece serviços de valor acrescentado em Cibersegurança, que combinam o seu know-how e tecnologia proprietária para reduzir, de forma consistente e eficaz, o risco cibernético dos seus clientes.

As gamas de serviços abrangentes incluem Testes de Intrusão Persistentes, Consultoria e Soluções de ISO 27001, PCI-DSS, GRC e gestão de riscos de terceiros.



Having the ambition to make the difference and the passion for Cybersecurity was what moved me to go ahead with Integrity. But that's not enough by far. Having the right team, the persistence for doing it right and generating value-added in the Industry along with great clients was key for the achievement. – **Rui Shantilal, Managing Partner**

INTRODUÇÃO

TOP VULNERABILIDADES E RECOMENDAÇÕES

Com uma estrutura simples e clara, o **Overview 2021 - Top Vulnerabilidades e Recomendações** da INTEGRITY pretende dar a conhecer, através da análise dos principais indicadores, os dados dos seus clientes a nível nacional e internacional, relativos às vulnerabilidades identificadas no ano passado, no âmbito do serviço de KEEP-IT-SECURE-24.

Centrando-se essencialmente em três grandes setores de atividade económica - Financeiro, Indústria & Energia e Serviços - este relatório disponibiliza informação referente à incidência de vulnerabilidades, nível, evolução de severidade e respetivos impactos, acompanhados de um conjunto de recomendações com medidas preventivas face a potenciais ataques.

Olhando para trás, se 2020 foi um ano absolutamente imprevisível e atípico pelas profundas mudanças a que a situação pandémica obrigou, é indubitável que 2021 foi igualmente desafiante para todos os setores. Apesar de passado o desafio inicial, perante a necessidade de adaptação a uma nova realidade, ficou claro que a dinâmica do mercado nunca mais seria a mesma e que a estratégia de crescimento de qualquer organização teria inevitavelmente de continuar a incluir o digital, tendo sido, aliás a tecnologia a garantir a continuidade de muitos negócios.

Em 2021, as plataformas digitais e o teletrabalho deixaram de ser novidade - a maioria das projeções têm mesmo vindo a demonstrar que o futuro do trabalho é híbrido - no entanto, apesar dos inúmeros benefícios apontados tanto para colaboradores como para entidades empregadoras, a verdade é que ficámos todos mais vulneráveis e expostos, o que acaba por comprometer a segurança da informação não só das empresas e dos clientes, mas de toda a cadeia de comercialização.





Os ataques cibernéticos são atualmente uma das maiores ameaças às empresas e a sua frequência, intensidade e sofisticação têm aumentado. Em 2021, a Gartner afirmou que os serviços de segurança, incluindo serviços de consultoria, implementação e outsourcing, seriam responsáveis pela categoria de gastos mais elevados, sendo que segundo o Gartner 2021 CIO Agenda Survey¹, 61% dos mais de 2000 CIO's entrevistados aumentaram o investimento em cibersegurança².

Não há dúvida que vivemos tempos exigentes, num cenário de iminentes mudanças que nos presenteiam com mais dúvidas do que certezas, mas há um caminho a fazer: o da prevenção e aposta na Segurança da Informação, a qual consiste na implementação de vários processos e controlos de segurança, de forma continuada, com o intuito de identificar eventuais riscos e vulnerabilidades técnicas e, desta forma, ajudar os clientes a proteger a sua informação.

De referir, por último, que os dados seguidamente expostos foram tratados de forma totalmente confidencial e que os outliers não foram tidos em conta, por apresentarem valores bastante diferentes de todos os outros e poderem enviesar os resultados seguidamente apresentados.

-
1. <https://www.gartner.com/en/newsroom/press-releases/2021-05-17-gartner-forecasts-worldwide-security-and-risk-managem>
 2. <https://www.gartner.com/en/newsroom/press-releases/2020-10-20-gartner-survey-of-nearly-2000-cios-reveals-top-performing-enterprises-are-prioritizing-digital-innovation-during-the-pandemic>

PENTESTING

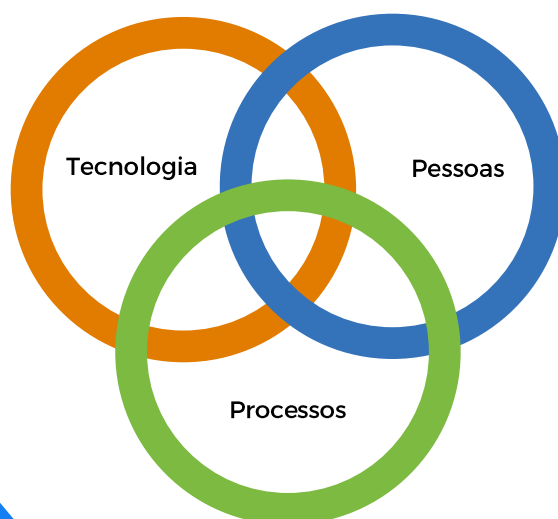
A evolução da Segurança da Informação, fator crítico de negócio, pode ser alcançada através do alinhamento entre estes 3 elementos: Tecnologia + Pessoas + Processos

Nas últimas décadas, o digital tem ganho uma força e um protagonismo tal, sendo quase impensável concebermos um modelo de negócio que não inclua esta vertente.

A transformação digital trouxe consigo novos conceitos e oportunidades, acarretando igualmente grandes desafios que “obrigaram” certas empresas a reinventar-se, para conseguirem responder e estar à altura das necessidades e exigências do mercado e dos clientes.

Ora, neste contexto, perante o crescimento da interconectividade entre ambientes de trabalho, a informação e os dados das empresas ficaram inevitavelmente mais expostos. Esta exposição e vulnerabilidades associadas criaram o cenário perfeito para os hackers - através de estratégias cada vez mais sofisticadas, imprevisíveis e rápidas - entrarem em ação.

Os alvos tanto são grandes e mediáticas empresas, como PME's, que devem envolver, o quanto antes, a questão da cibersegurança no processo de tomada de decisão. Esta deve ser considerada numa estratégia de sustentabilidade e crescimento, com tomada de consciência tanto ao nível operacional como de gestão.





O QUE FAZER ENTÃO?

Identificar os riscos, vulnerabilidades, grau de exposição e o nível de conformidade das suas práticas de **Gestão da Segurança da Informação**, de forma a conhecerem detalhadamente os riscos.

COMO?

Através da realização dos **Testes de Intrusão Pontuais ou Persistentes (Penetration Tests)**, feitos geralmente por entidades independentes e externas, com periodicidade anual ou semestral ou mesmo permanente que têm como fim testar precisamente as defesas dos sistemas e aplicações aos olhos de um potencial atacante.

Através de metodologias e ferramentas próprias, os consultores atuam como se se tratassem de potenciais atacantes e identificam assim as fragilidades existentes. No final, é apresentado um relatório com os resultados descritos e as recomendações de correção.

Um aspeto a não descurar é também a relação entre três importantes elementos e que são os pilares de qualquer organização: **Tecnologia, Pessoas e Processos**, cuja interação é essencial para garantir o sucesso das estratégias delineadas, no âmbito da Gestão da Segurança da Informação.

Na verdade, dentro de qualquer organização há que unir esforços de forma a manter um equilíbrio entre as **Pessoas** - consciencializando os utilizadores para atuarem como uma espécie de extensão das equipas de cibersegurança - e investir e manter não só a Tecnologia sempre atualizada, como optar pelo uso de **Processos** adequados e robustos de gestão de cibersegurança.

KEEP-IT-SECURE-24 OVERVIEW

Testar, de forma continuada e persistente, o impacto das alterações na sua Segurança, através de ferramentas e metodologias como se tratasse de um potencial atacante.

Aumento da eficiência, agilidade e produtividade, oportunidade para inovar, maior competitividade, clientes mais satisfeitos, redução de custos... estas são apenas algumas das vantagens que a transformação digital trouxe às empresas, revolucionando, por completo, o mundo dos negócios.

No entanto, a par disto vieram também riscos e aspetos menos positivos, encontrando-nos agora mais expostos perante um mercado global, aberto e imensamente rápido na forma de agir.

A maioria dos negócios estão digitalizados e os processos automatizados, o que significa que estão mais vulneráveis a possíveis ataques. Empresas e colaboradores têm de estar cientes disto e devem, mais do que nunca, procurar sempre manter a integridade da informação por si processada. É imperativo que os dados sejam protegidos e mantidos em segurança, no que respeita à sua confidencialidade, integridade e disponibilidade.

De forma a ter noção do real impacto e consequências para toda a empresa caso os seus sistemas sofressem um ataque, poderá optar por testar a sua segurança, de forma regular e continuada, num modelo eficiente ao nível de custos em formato de Serviços Geridos.

Isto é possível graças ao **KEEP-IT-SECURE-24**, o qual eleva os testes de intrusão a um novo patamar porque, para além de realizar testes continuados e persistentes, disponibiliza uma Plataforma de Gestão online onde os clientes podem gerir os seus ativos e vulnerabilidades associadas, extrair relatórios e obter métricas de risco.





O KEEP-IT-SECURE-24 providencia serviços continuados ao nível dos Testes de Intrusão, por parte de uma equipa profissional de auditores qualificados e certificados para o efeito.



Customizados de acordo com as necessidades e objetivos do cliente, este tipo de projeto tanto pode ser mais orientado para a componente **técnica**, **processos e pessoas**, como para outros âmbitos mais específicos.



Gerir KPIs



Fazer cumprir Timings de Resolução



Integrar com a Gestão de Alterações



Extrair Relatórios Dinâmicos



Estabelecer Prioridades de Testes



Testar Cenários Avançados



Monitorizar Aplicações e a Performance das Equipas em termos de Gestão de Vulnerabilidades



Analisar e Incorporar Lições Aprendidas



PROCESSO DE TESTES

Tendo como alvo os sistemas e aplicações dos clientes, o processo de testes é extremamente importante, pois permite uma identificação objetiva de potenciais problemas, vulnerabilidades e riscos associados, viabilizando que as organizações efetuem, com tempo e de forma efetiva, a gestão e redução do risco.



PENTESTING OVERVIEW 2021

ENQUADRAMENTO DAS MÉTRICAS

ENTIDADES

No portefólio de entidades clientes da INTEGRITY consta um alargado leque com referências, tanto no mercado nacional como internacional, entre médias e grandes empresas dos mais variados setores, desde a banca e seguros, retalho, energia, saúde, organismos públicos, entidades governamentais, telecomunicações, aviação entre outros.

Apesar dos ataques cibernéticos terem impactos irreparáveis em todos estes setores e com enormes prejuízos a vários níveis, nomeadamente financeiros, o presente relatório debruçar-se-á sobre **3 grandes setores de atividade económica**:



SETOR FINANCEIRO

Por norma, é um dos setores mais maduros na aplicação de práticas de cibersegurança, por um lado por ter sido um dos primeiros a ser alvo deste tipo de ataques, por outro, pelo facto das regulamentações e obrigações estarem numa fase mais madura do que noutros setores.



SETOR INDÚSTRIA & ENERGIA

Este setor engloba grandes organizações, cujas ameaças e riscos de cibersegurança tendem a aumentar cada vez mais, condicionando o normal funcionamento dos seus serviços e operações.



SETOR DOS SERVIÇOS

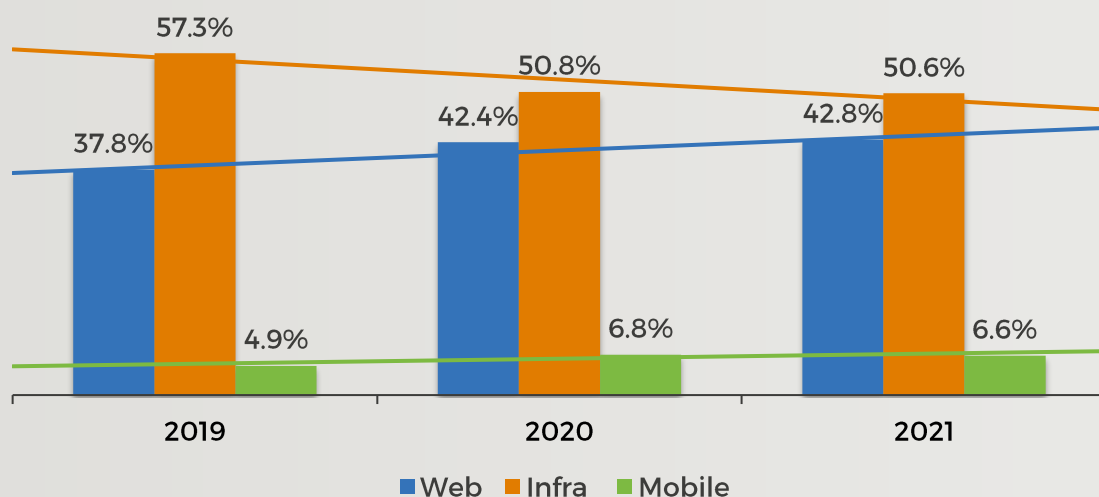
Um setor bastante vasto onde se incluem diversas entidades, cada uma com diferentes graus de exposição, sendo imprescindível uma aposta na segurança da informação pelo profundo impacto que poderá causar no negócio e na sua continuidade.

SOBRE OS ASSETS

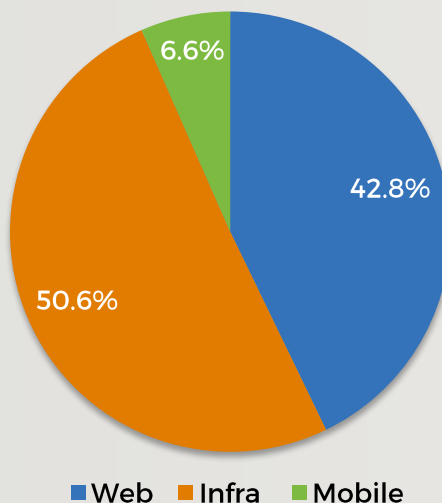
Os assets (ativos) são sistemas, redes ou aplicações visadas pelo Serviço de Pentesting.

No âmbito do KEEP-IT-SECURE-24, o Pentesting executado em 2021 incidiu essencialmente sobre os 3 tipos de assets apresentados no gráfico abaixo: com a percentagem mais elevada (50.6%) temos a Infraestrutura, de seguida a Web (42.8%) e o Mobile (6.6%).

EVOLUÇÃO DE ASSETS DE 2019 A 2021



DISTRIBUIÇÃO DOS TIPOS DE ASSETS



TENDÊNCIAS

De acordo com o gráfico, podemos observar que nos últimos três anos se registou uma tendência de crescimento na vertente de Web, ao contrário das Infraestruturas que de 2019 para 2020 decresceram, mantendo-se iguais em 2021 e do Mobile que registou um aumento de 2019 para 2020 e se manteve em 2021.

O aumento de assets na vertente de Web segue uma tendência natural de crescimento e está de igual forma relacionado com o crescimento de exposição de serviços online que aumentou substancialmente com a pandemia.

O decréscimo verificado nas Infraestruturas justifica-se em parte pela tendência de migração para a serviços em Cloud, em vez da abordagem tradicional de servidores físicos. Nestas situações, é aplicável um modelo de Shared Responsibility em que a responsabilidade de alguns componentes é partilhada entre o cliente e o fornecedor de serviços Cloud, dependendo do modelo de entrega de serviço. A responsabilidade sobre a segurança da perspetiva do cliente decresce substancialmente nos modelos PaaS e SaaS.

Por outro lado, as tendências de aumento de aplicações web e o decréscimo de assets de infraestrutura visados pelos testes, refletem também alguma centralização na publicação de aplicações web em equipamentos de balanceamento e segurança.

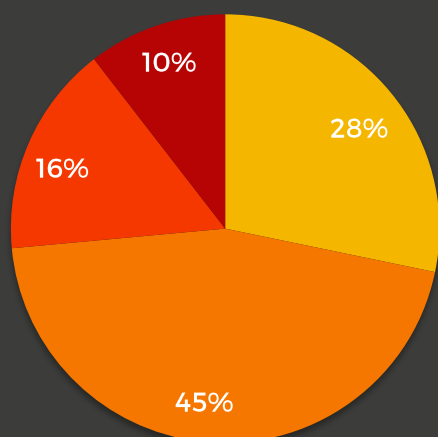
Podemos observar com base nos 3 gráficos de distribuição de severidades por tipo de asset que as aplicações web e mobile registaram maior incidência de vulnerabilidades críticas e high, devido provavelmente à sua complexidade e também porque parte delas são desenvolvidas por medida em diversos clientes.

Os assets de Infraestrutura acabam por registar uma menor incidência de vulnerabilidades Critical e High devido ao facto de a maioria das organizações conseguir implementar soluções e processos de gestão de patches garantindo uma maior estabilidade, segurança e controlo de versões das aplicações e serviços que servem a organização.



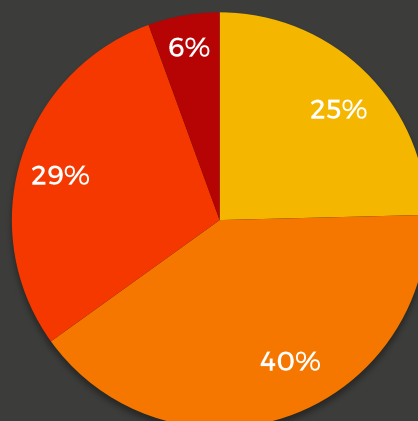
SEVERIDADE ASSETS

ASSETS WEB - SEVERIDADE



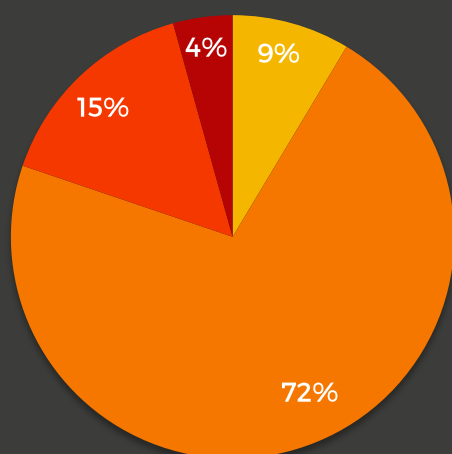
■ Low ■ Medium ■ High ■ Critical

ASSETS MOBILE - SEVERIDADE



■ Low ■ Medium ■ High ■ Critical

ASSETS INFRA – SEVERIDADE



■ Low ■ Medium ■ High ■ Critical



VULNERABILIDADES

Nos últimos anos, seja a nível nacional ou internacional, as organizações têm vindo a sofrer cada vez mais ciberataques, traduzindo-se muitos destes episódios em enormes prejuízos e danos, que afetam inevitavelmente a atividade dita normal dessas mesmas organizações.





Devido ao aumento da presença da tecnologia nas nossas vidas, ficámos todos - cidadãos e organizações - mais vulneráveis a eventuais falhas nos sistemas de informação e tecnologia, daí a tónica à volta do tema da Segurança da Informação.

Os ciberataques o que fazem é precisamente explorar vulnerabilidades de segurança, com o intuito de assumir o controlo ou interromper a funcionalidade dos processos, e é por isso que é importante identificar e analisar essas vulnerabilidades.

As vulnerabilidades apresentam vários níveis de severidade e, conforme esse nível, existem práticas de resolução específicas que ajudam a detetar e, desde que atempadamente, a solucionar o problema.

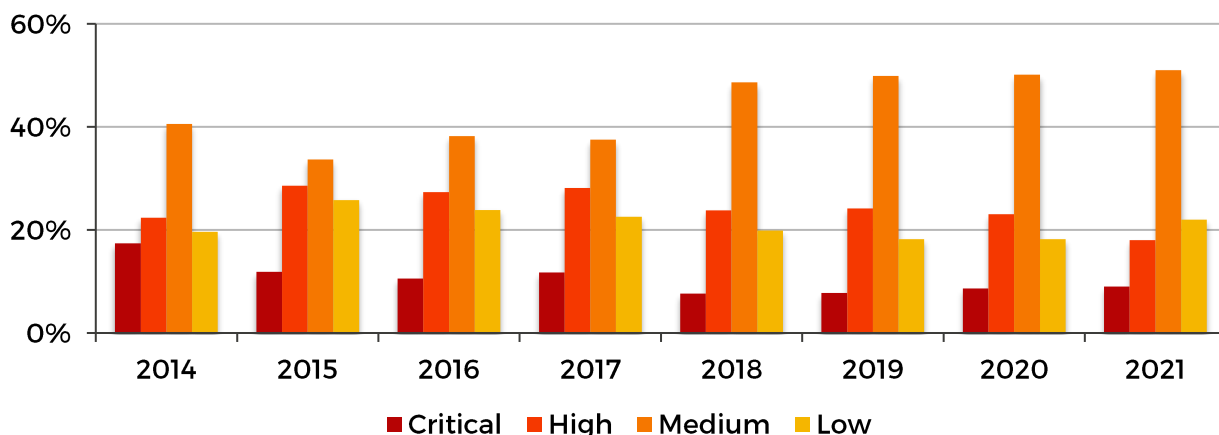
SEVERIDADE DAS VULNERABILIDADES

Tal como se pode constatar abaixo, a tipologia de severidade das vulnerabilidades está dividida em 4 níveis: **LOW, MEDIUM, HIGH E CRITICAL**.

Severidade	Critério
 Critical	Vulnerabilidades que apresentam risco iminente e grave para a informação ou sistemas.
 High	Vulnerabilidades que apresentam risco para a informação ou sistemas, mas a exploração apresenta restrições e o impacto não é completo em todos os vetores.
 Medium	Vulnerabilidades que requerem esforço adicional ou informações adicionais para serem exploradas e o impacto é reduzido.
 Low	Vulnerabilidades que por si só não causam impacto, mas podem ser usadas para ajudar na descoberta e exploração de outras vulnerabilidades.

É de referir que as severidades do nível **HIGH** ou **CRITICAL** significam que o impacto potencial nos sistemas ou informação é elevado.

EVOLUÇÃO DA SEVERIDADE POR VULNERABILIDADES DE 2014 A 2021



O gráfico acima mostra que, ao longo dos últimos oito anos, apesar de ténue há tendência de decréscimo nas vulnerabilidades Critical, o que demonstra um aumento crescente na perceção do risco e maturidade por parte de algumas das empresas visadas pelos testes.

Ainda em relação às vulnerabilidades Critical, verifica-se que a sua percentagem, face ao total de vulnerabilidades identificadas em 2021, se encontra ao mesmo nível de 2020, observando-se o mesmo nas vulnerabilidades Medium.

Quanto às vulnerabilidades High, houve um decréscimo de 5% que aparenta estar relacionado com as descidas registadas nos três tipos de vulnerabilidades High mais comuns, nomeadamente o Sensitive Data

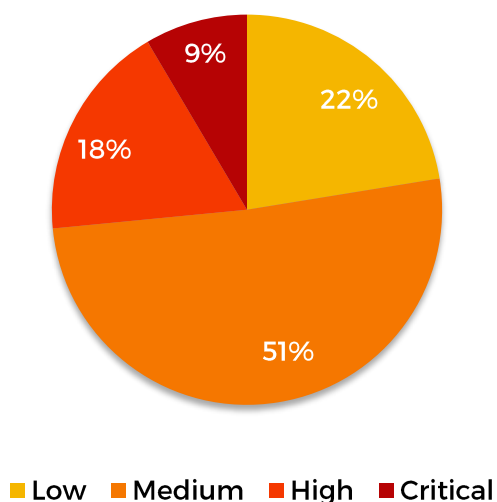
Exposure (-6%), o Cross Site Scripting (-2%) e o Security Misconfiguration (-2%).

É possível verificar um aumento das vulnerabilidades Low em 4% de 2020 para 2021, o que provavelmente se deve ao aumento das vulnerabilidades de Broken Authentication and Session Management. É interessante verificar que a utilização do serviço de Pentesting regular leva a um decréscimo ao longo do tempo das vulnerabilidades High e Critical, bem como um aumento da agilidade na sua resolução. A natureza regular das interações de discussão das vulnerabilidades encontradas, leva a que os clientes iniciem ou otimizem os seus processos internos de gestão de segurança, desenvolvimento e deteção de vulnerabilidades.



DISTRIBUIÇÃO DAS VULNERABILIDADES POR SEVERIDADE NO DECORRER DE 2021

Tal como se pode verificar no gráfico, há manifestamente uma maior percentagem nas vulnerabilidades com severidade Medium (51%), pois são aquelas que refletem temas de menor impacto e até mesmo de exploração pouco útil para o atacante.

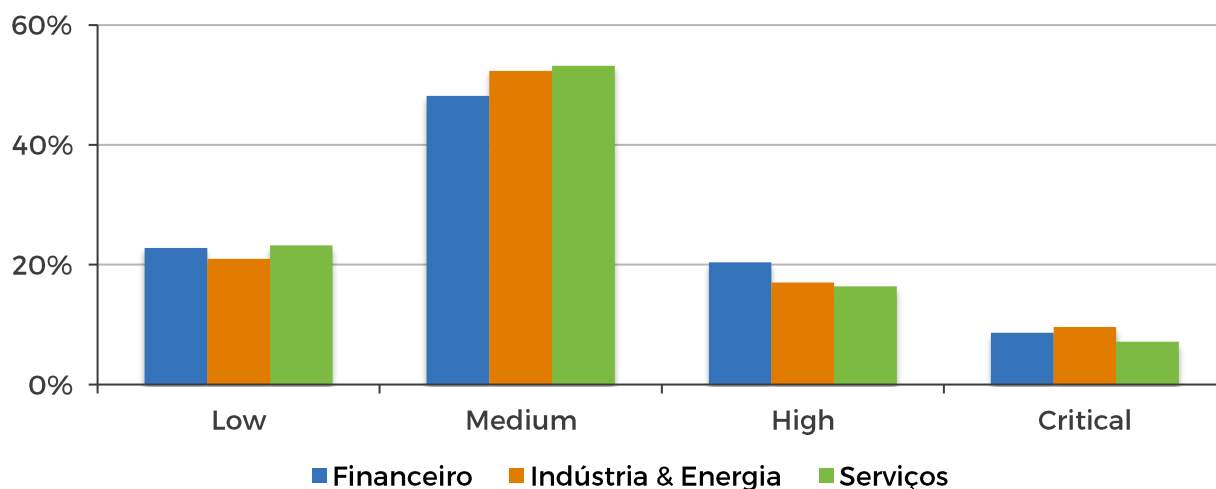


É de chamar a atenção para as vulnerabilidades com severidade Critical que, apesar de registarem um valor na ordem dos 9%, é por si só significativo pelo impacto causado por este tipo de severidade que é normalmente muito grave, podendo traduzir-se em danos na reputação das empresas, perda de clientes, contratos, receitas e oportunidades de negócio, ou seja, perdas avultadas e, por vezes, irreparáveis. É o chamado “efeito dominó” que acaba por minar e afetar toda a organização.

Por tudo isto, nos dias que correm e face a estas consequências devastadoras, uma eficiente gestão dos riscos cibernéticos deverá ser prioridade para qualquer organização.



DISTRIBUIÇÃO DE SEVERIDADE POR SETOR: FINANCEIRO, INDÚSTRIA & ENERGIA E SERVIÇOS



Tal como se pode constatar no gráfico, o setor dos Serviços foi o que se destacou pela positiva em 2021 atendendo a que é o que apresenta a menor percentagem no número de vulnerabilidades de severidades Critical identificadas, comparando com os outros setores, tendo registado um decréscimo de 5% neste tipo de severidade em relação ao ano passado.

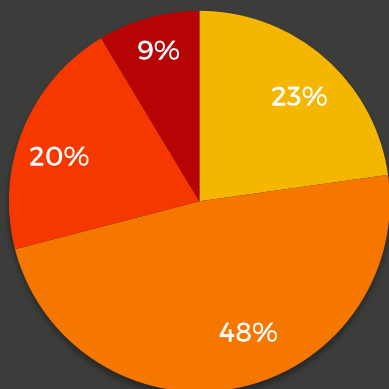
Ainda no que diz respeito às vulnerabilidades com severidade Critical, os setores Financeiro e Indústria & Energia mantêm-se em linha com o ano de 2020, registando apenas um aumento de 2% e 1%, respetivamente.

Olhando para as vulnerabilidades com severidade High, verifica-se que todos os setores contribuíram para o decréscimo global desta severidade, sendo, no entanto, de assinalar que em 2021 o setor dos Serviços é o que regista maior descida: 9% em relação a 2020.

É de referir ainda que, apesar do crescimento dos serviços disponibilizados online, se observou uma maior preocupação em relação à sua segurança, que pode ser comprovada com o decréscimo de 5% e 9% em relação às vulnerabilidades Critical e High, respetivamente.

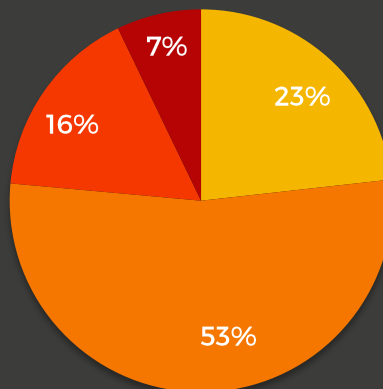


SEVERIDADE NO SETOR FINANCEIRO



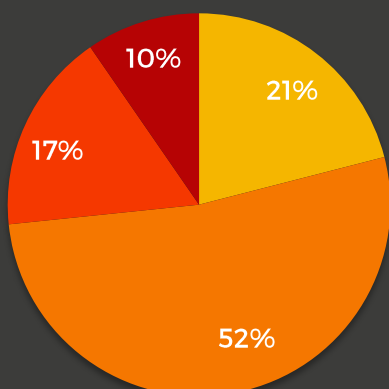
■ Low ■ Medium ■ High ■ Critical

SEVERIDADE NO SETOR DOS SERVIÇOS



■ Low ■ Medium ■ High ■ Critical

SEVERIDADE NO SETOR INDÚSTRIA & ENERGIA



■ Low ■ Medium ■ High ■ Critical



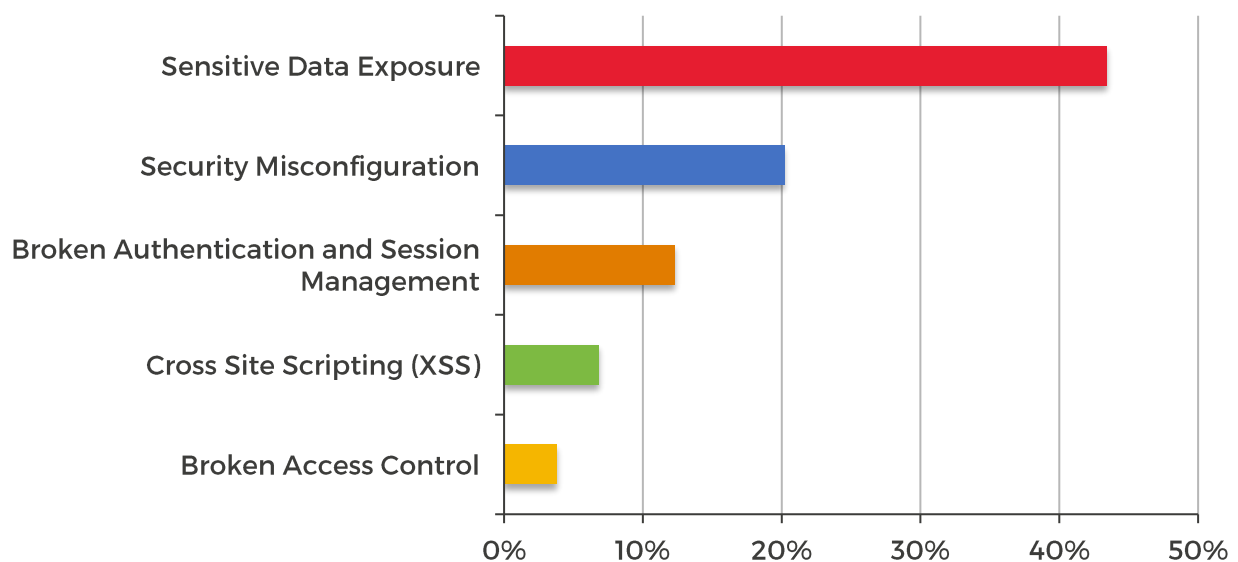


TOP 5 TIPOS DE VULNERABILIDADES

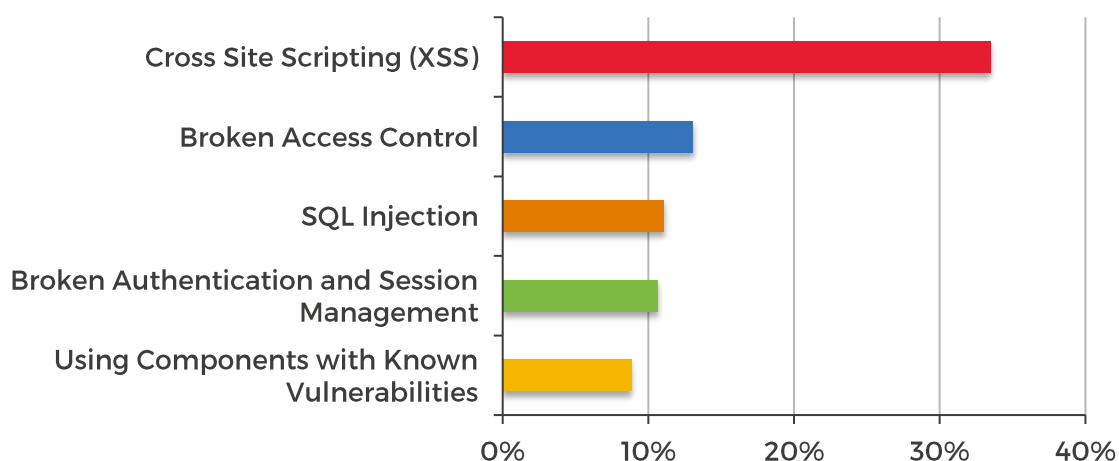
TIPOS DE VULNERABILIDADES MAIS COMUNS – 2021

O gráfico mostra o Top 5 de tipos de vulnerabilidades mais comuns em 2021, encontrando-se em linha com as vulnerabilidades identificadas em 2020.

Como se pode verificar, ao longo de 2021 o **Sensitive Data Exposure** foi efetivamente a vulnerabilidade mais comum presente em todo o leque de clientes da INTEGRITY.



TIPOS DE VULNERABILIDADES CRÍTICAS MAIS COMUNS – 2021



Neste gráfico estão os **Tipos de Vulnerabilidades Críticas mais Comuns** em 2021.

Podemos constatar ao olhar para os 2 gráficos que existem vários tipos de vulnerabilidades que se encontram presentes em ambos, ou seja, para além de serem comuns entre as vulnerabilidades de severidade crítica também são comuns no universo geral de vulnerabilidades.



SENSITIVE DATA EXPOSURE

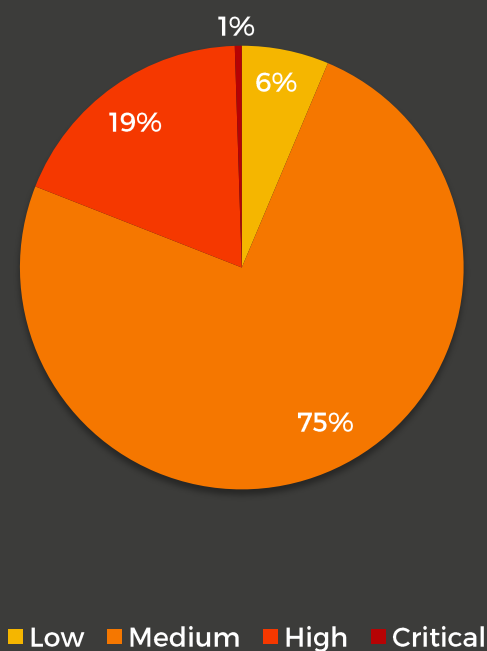
Os chamados dados confidenciais ou informação sensível - que pode incluir informações tão variadas como identificação pessoal, números referentes a contas bancárias, cartões de crédito, seguros, saúde, chaves criptográficas, notas confidenciais, etc.- é informação que deve ser protegida, em trânsito, repouso ou processamento, contra qualquer acesso que não seja autorizado. Ora, o **Sensitive Data Exposure** ocorre quando este tipo de informação não é devidamente protegida, sendo que este tipo de vulnerabilidade acontece maioritariamente devido à ausência ou mesmo erros na configuração do protocolo de segurança Transport Layer Security (TLS), cuja finalidade é garantir e facilitar a privacidade e integridade de dados em trânsito.

Apesar da maioria das pessoas estar ciente da importância deste protocolo, a verdade é que ainda se verificam bastantes vulnerabilidades na implementação deste protocolo, nomeadamente com a utilização de cifras fracas, o que permite aos atacantes ultrapassar este importante mecanismo de proteção.

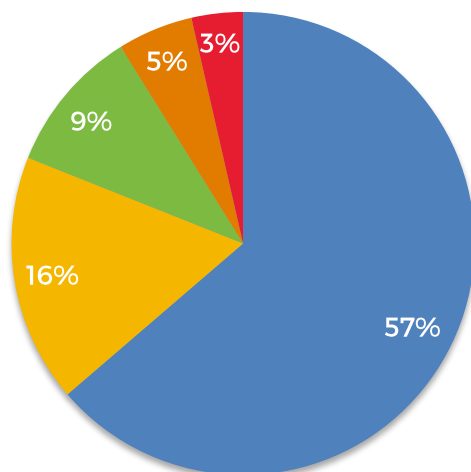
Como se pode constatar, a Utilização de Cifras Fracas (cifras consideradas vulneráveis ou pouco seguras) e Problemas com certificados são as classes mais comuns, com 73% do total de vulnerabilidades de Sensitive Data Exposure.

A falta dos cabeçalhos de segurança como o HSTS e Credenciais em Claro, maioritariamente em testes Web, representam 9% e 3%, respetivamente e Renegociação do lado do cliente com os restantes 5%.

SENSITIVE DATA EXPOSURE – SEVERIDADE



SENSITIVE DATA EXPOSURE – SUBTIPO



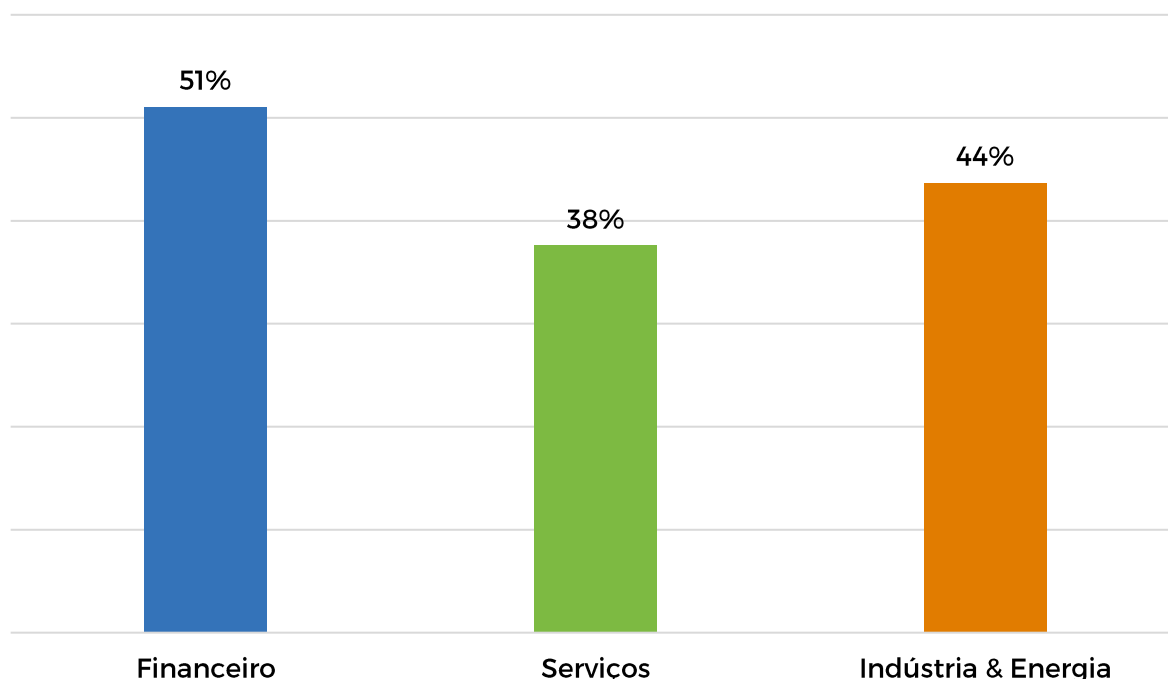
■ Weak Ciphers ■ Certificate Issues ■ Security Headers ■ Client Renegotiation Enabled ■ Credentials Cleartext

O cabeçalho Strict-Transport-Security (HSTS) garante que o site seja sempre acessado por HTTPS e impede que o utilizador aceite certificados inválidos para aceder à aplicação. Esta medida visa proteger contra ataques de Man-in-the-Middle (MitM). Trata-se uma medida simples de implementar, sem impacto no desenvolvimento das aplicações, devendo apenas ser garantida a validade dos certificados implementados para acesso à aplicação e a configuração de um parâmetro de expiração adequado à aplicação em causa.

É de mencionar que as Credenciais em Claro englobam todas as situações em que as credenciais dos utilizadores sejam transmitidas pela rede, sem estarem cifradas. Esta vulnerabilidade representa um risco acrescido, uma vez que permite o takeover a contas de utilizadores, através do acesso às credenciais armazenadas ou através de ataques MitM, capturando as credenciais ou variáveis de sessão transmitidas em claro na rede.



SENSITIVE DATA EXPOSURE – SETOR



Considerando que estamos a observar dados relativos à categoria de vulnerabilidades mais comum, não é de estranhar a grande relevância de vulnerabilidades em cada setor. Das vulnerabilidades identificadas no setor Financeiro, 51% são Sensitive Data Exposure. O setor da Indústria & Energia atinge os 44% e o setor de Serviços 38%.

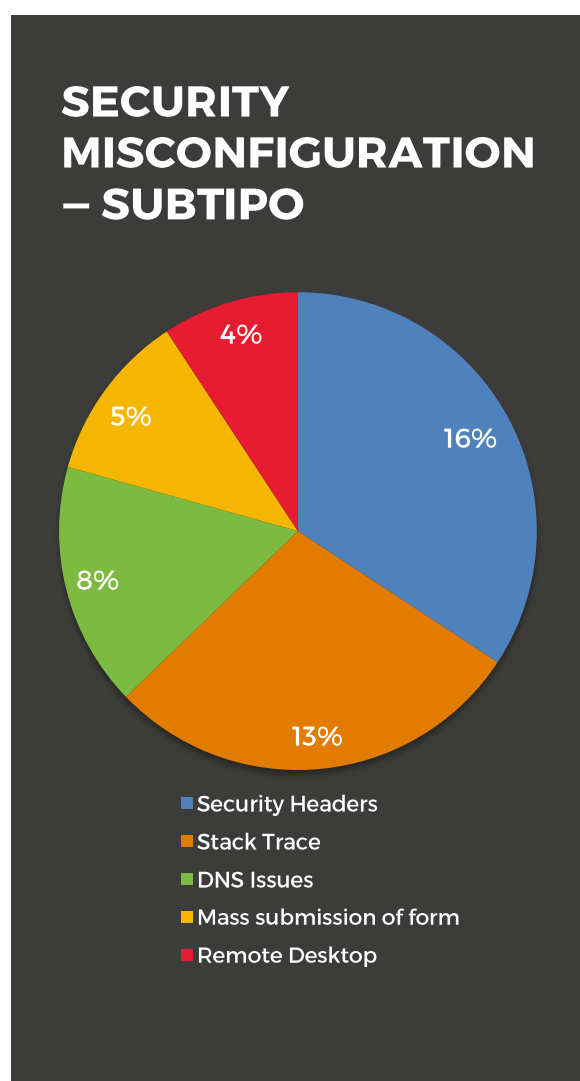
Apesar de a diferença entre setores não ser significativa, podemos observar com maior frequência no setor Financeiro e Indústria & Energia a necessidade de retrocompatibilidade, o que implica a utilização de algumas cifras não recomendadas que, por seu turno, se traduzem em vulnerabilidades publicadas.

Recomendações

- *Classificação da informação armazenada e transmitida por cada aplicação para garantir que os dados sensíveis são identificados, cumpridos todos os requisitos legais e de negócio e que são aplicados os controlos adequados.*
- *Utilização de algoritmos fortes e standard para o transporte e armazenamento da informação.*
- *Definição de diretivas internas relativamente a protocolos e cipher-suites suportados, tendo em consideração os requisitos de negócio, a sensibilidade da informação e suporte desejado aos utilizadores finais das aplicações.*
- *Não reter dados sensíveis que não sejam estritamente necessários ao funcionamento da aplicação/serviço.*
- *Verificar a eficácia das definições e configurações implementadas, de forma independente.*

SECURITY MISCONFIGURATION

O segundo tipo de vulnerabilidade mais comum é o **Security Misconfiguration**, o qual engloba configurações incorretas em várias vertentes como error handling, hardening, default configuration, com especial prevalência em aplicações web. Este tipo de problema surge quando as melhores práticas de segurança não são seguidas, nomeadamente em situações como a ausência de hardening, utilização de configurações default, funcionalidades de debug ou de qualidade, que depois não são desativadas quando os sistemas são colocados em produção, ausência de headers de segurança entre outras.

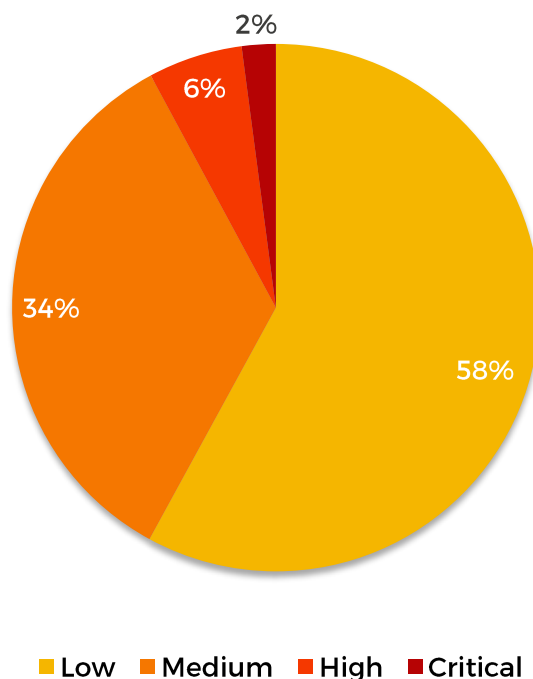


No que diz respeito a esta vulnerabilidade no decorrer de 2021, pode-se observar que no top 5 temos os Headers de Segurança com 16% de incidências, seguindo-se a visualização do Stack Trace com um valor também significativo (13%), os problemas de configuração de DNS, a submissão massiva de forms e, por fim, as configurações de Remote Desktop.

Tal como já referido anteriormente, com a pandemia o trabalho remoto passou de uma situação emergente para uma situação dita de normalização, com muitas organizações a assumir o novo modelo de trabalho à distância ou híbrido. Desta forma, é exetável que tecnologias de trabalho remoto comecem a representar uma tendência crescente nas vulnerabilidades identificadas, como é o caso do Remote Desktop.



SECURITY MISCONFIGURATION – SEVERIDADE

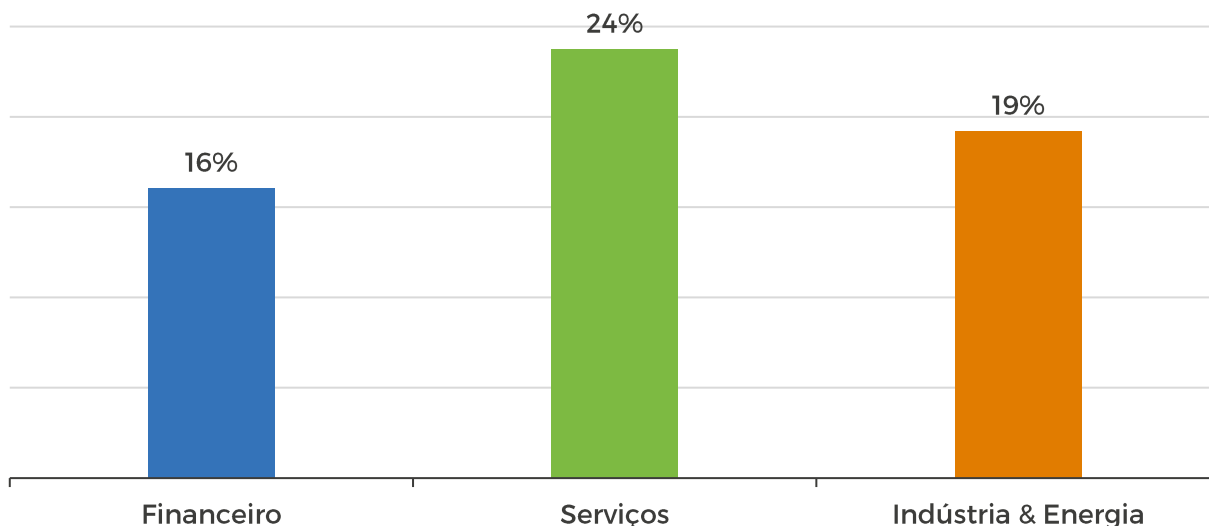


Tal como demonstra o gráfico, as vulnerabilidades de **Security Misconfiguration** encontram-se dispersas por todas as severidades, sendo que cerca de 92% são de severidade Medium e Low, igual ao que aconteceu em 2020 cuja percentagem foi ligeiramente mais baixa.

Só uma nota a reter, como se pode ver no gráfico o valor da severidade Critical neste tipo de vulnerabilidades é residual (2%), no entanto isto não significa que não haja situações de grande gravidade, pelo contrário, verificou-se a existência de credenciais de administração por omissão, credenciais nos Stack Traces, ficheiros de backup disponíveis publicamente, possibilidade de escalada de privilégios ou possibilidade de Denial of Service (DoS). Podemos concluir que neste tipo de vulnerabilidade, a probabilidade de uma ocorrência severa é baixa mas, quando acontece, o impacto é bastante elevado.



SECURITY MISCONFIGURATION – SETOR



Relativamente à distribuição por setores, consegue-se verificar um claro destaque para o setor de Serviços com aproximadamente 24% das suas vulnerabilidades serem Security Misconfiguration, comparativamente com o setor Financeiro com 16% e da Indústria com 19%.

Estes valores estão em linha com as expectativas, considerando que os setores Financeiro e Indústria & Energia têm uma menor heterogeneidade de aplicações Web e maior estabilidade de ambientes ao longo do tempo, contrastando com o setor dos Serviços com uma tendência para novas aplicações incrementalmente mais complexas, cuja configuração requer curvas de aprendizagem por parte das equipas técnicas.

Recomendações

- *Aplicar controlos de segurança a todos os servidores e aplicações. O Center for Internet Security fornece uma checklist de controlos de segurança a implementar e pode ser um bom ponto de partida para as organizações.*
- *Ter ambientes distintos de desenvolvimento, qualidade e produção, com configurações e credenciais independentes. Idealmente, o processo de Deployment destes ambientes deve estar automatizado de forma a minimizar erros durante o processo.*
- *Remover todas as funcionalidades, componentes e documentação que não seja estritamente necessário ao funcionamento do serviço em causa.*
- *Segurança do lado do cliente: enviar sempre as diretivas de segurança para os clientes, por exemplo: Security Headers.*
- *Implementar um processo regular de revisão e atualização das checklists de controlos de segurança a implementar.*



VULNERABILIDADES CRÍTICAS MAIS COMUNS

Embora ocorram com menor frequência, as vulnerabilidades com severidade Critical são as que causam mais prejuízos e com maior gravidade, levando mais rápida e facilmente a pôr em causa a segurança dos sistemas e aplicações.

O potencial impacto deste tipo de severidade é tal que não se pode, de forma alguma, descurar.

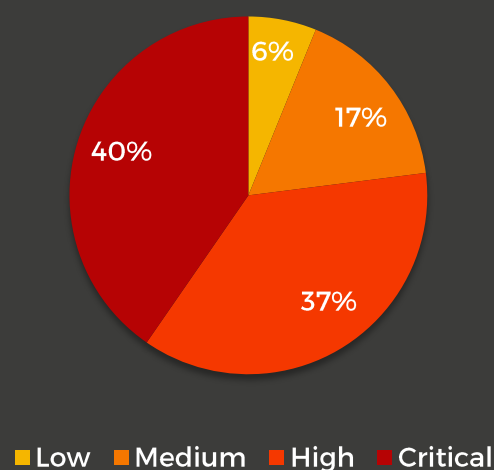
CROSS SITE SCRIPTING (XSS)

O **Cross Site Scripting** consiste na injeção de código JavaScript que é executado no browser da vítima no contexto da aplicação visada pelo ataque. Este tipo de vulnerabilidade é tipicamente usada para ganhar acesso ao cookie de sessão de um utilizador, levar um utilizador a executar ações na aplicação sem o seu conhecimento ou executar keyloggers no browser da vítima.

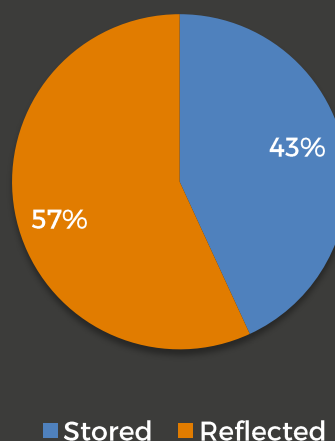
Existem dois tipos de **Cross Site Scripting**, o **Reflected** em que a vítima é manipulada para carregar num link que envia a payload maliciosa para a aplicação, e o **Stored**, em que a payload maliciosa fica guardada na aplicação e, a partir daí, todos os utilizadores que acedam à página que contém o código malicioso, serão comprometidos.

O **Stored Cross Site Scripting** tem tipicamente um impacto e severidade muito superior, mas a sua ocorrência também é inferior, representando 43% do total das vulnerabilidades identificadas, tal como demonstra o gráfico.

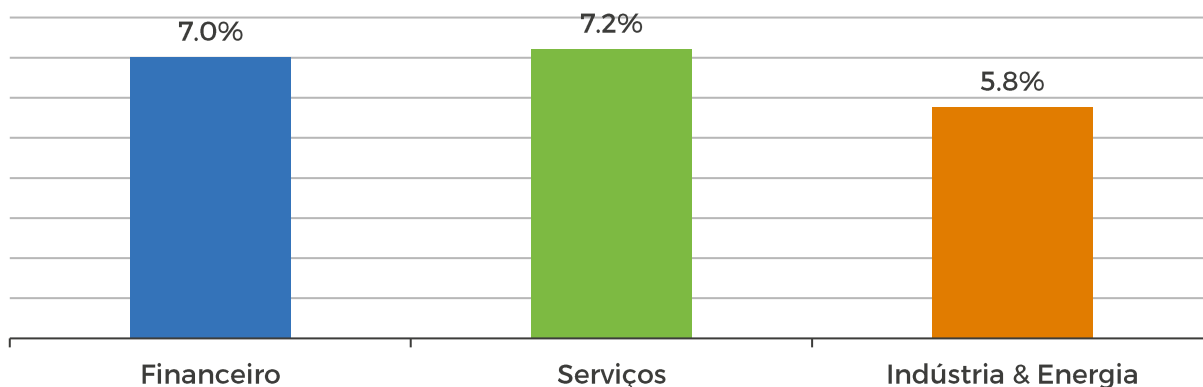
CROSS SITE SCRIPTING (XSS) – SEVERIDADE



CROSS SITE SCRIPTING (XSS) – SUBTIPO

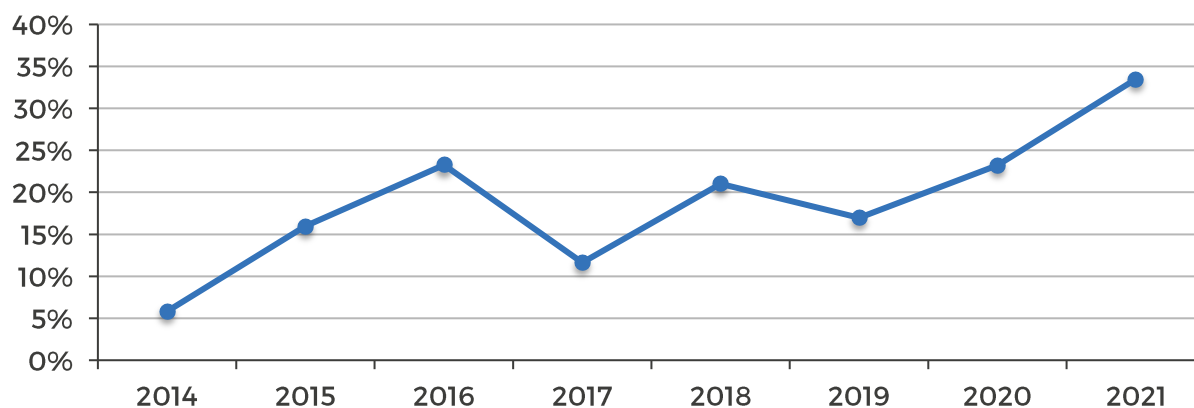


CROSS SITE SCRIPTING (XSS) – SETOR



Observando a percentagem de Cross Site Scripting por setor, verifica-se que a distribuição é bastante uniforme, com apenas uma diferença de 1,4% entre o setor da Indústria & Energia, que como já referido anteriormente, tem tipicamente com uma menor incidência em aplicações web e tendencialmente menos complexas, e o setor de Serviços.

Cross Site Scripting – Evolução



A análise de tendência ao longo dos últimos anos mostra uma subida bastante acentuada, com um crescimento de 10%, quando comparado com o ano de 2020.

Recomendações

- Dado o tipo de conteúdo que se espera que seja submetido, os dados introduzidos pelo utilizador devem ser rigorosamente filtrados nessa mesma base. Por exemplo, nomes devem apenas conter letras (acentos incluídos) e espaços, emails devem respeitar sempre a norma RFC 5322 (3.4.1. Addr-spec specification - pág.17), entre outros vários tipos de dados.
- Devem ser aplicados filtros de encoding e escaping do output para HTML, tais como OWASP, ESAPI ou Microsoft AntiXSSLibrary.
- O cabeçalho HTTP Content-Security-Policy deve ser definido de forma a que seja possível, por exemplo, executar apenas scripts disponíveis no domínio atual (script-src `self`) e negar scripts inline, bem como implementar sub resource integrity.

BROKEN ACCESS CONTROL

Naturalmente, e tal como o nome indica, a maioria das vulnerabilidades existentes nesta categoria dizem respeito a problemas de controlo de acesso. E o que é o controlo de acessos? É o mecanismo implementado, após a autenticação, que garante que a autorização de acesso aos conteúdos e funções presentes numa aplicação ou sistema, é permitida somente aos utilizadores adequados/supostos.

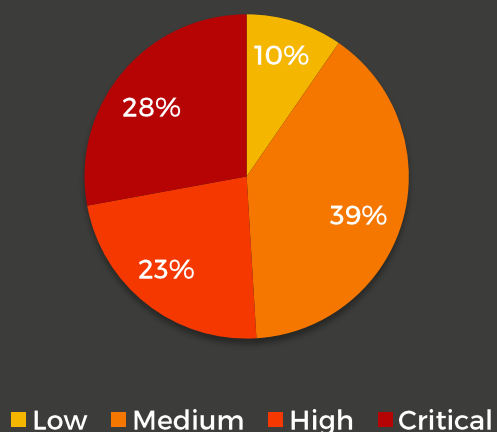
Esta implementação é algo complexa devido ao detalhe necessário na sua execução. De forma, a garantir que seja corretamente implementado, é necessário que todos os acessos, leitura, modificação ou eliminação de dados seja validado e garantido que o utilizador que solicita esta ação tem

autorização para o fazer. Este processo tem que ser feito transversalmente a toda a aplicação, o que aumenta a dificuldade da sua correta implementação proporcionalmente à complexidade da aplicação.

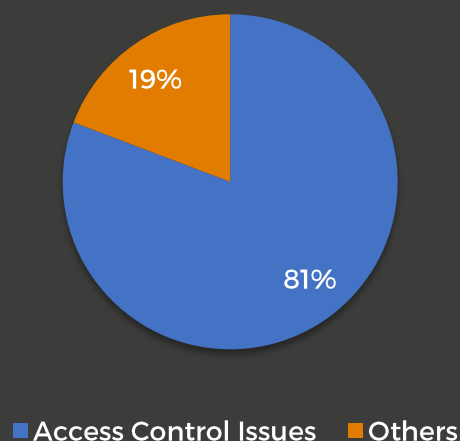
Como constatado, a possibilidade de escalada de privilégios e acesso/manipulação da informação de outros utilizadores, constituem mais de 80% das vulnerabilidades desta categoria.

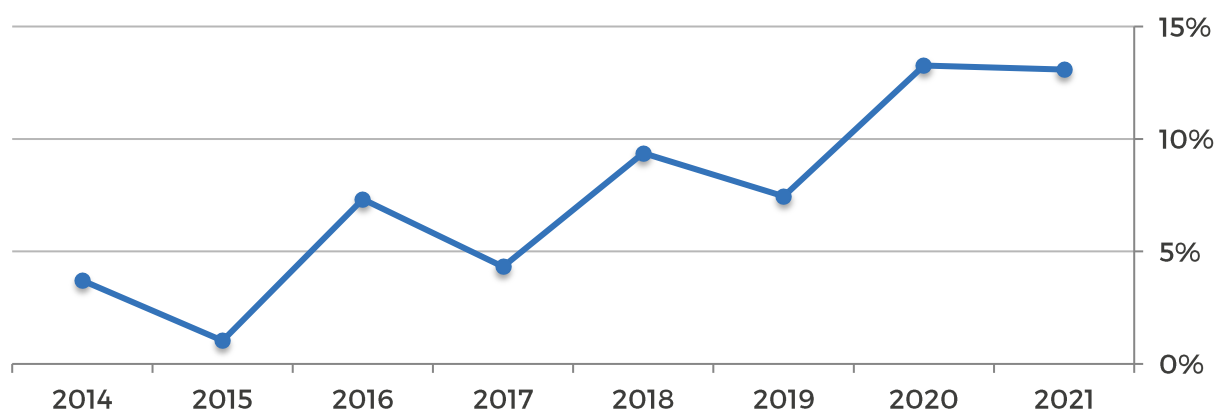
Apesar do decréscimo registado na ordem dos 28% a comparar com 50% referente a 2020 nas vulnerabilidades Critical, a tendência é de claro crescimento, com registo de duas subidas de 5% nos dois anos anteriores.

BROKEN ACCESS CONTROL – SEVERIDADE

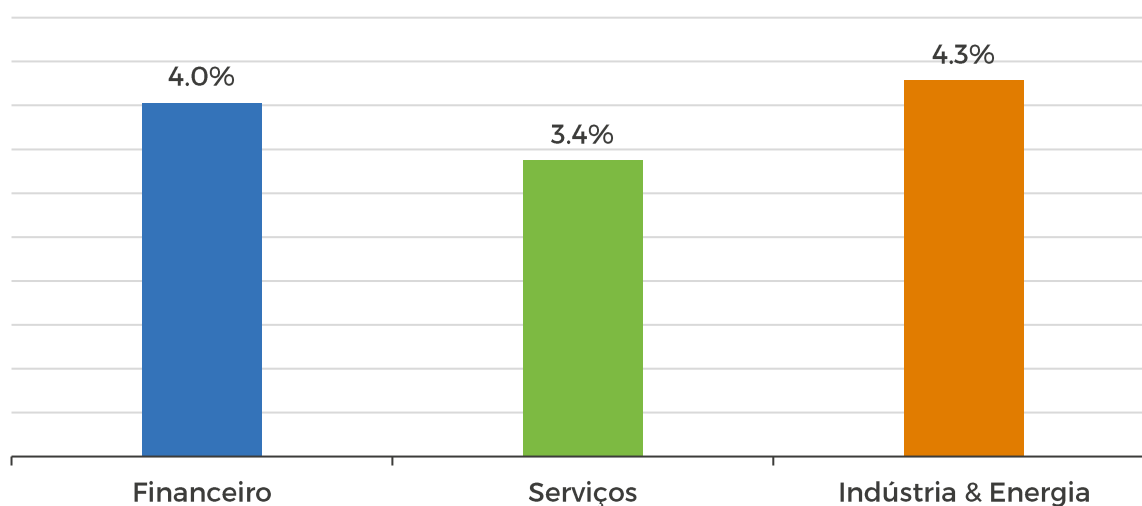


BROKEN ACCESS CONTROL – SUBTIPO



Broken Access Control – Evolução

BROKEN ACCESS CONTROL – SETOR



Quanto à percentagem deste tipo de vulnerabilidade por setor, a distribuição é também bastante uniforme, com apenas 0,9% de diferença entre os setores da Indústria & Energia com 4,3% e o dos Serviços com 3,4%. As vulnerabilidades de Broken Access Control do setor Financeiro, representam 4% do total de vulnerabilidades.

Recomendações

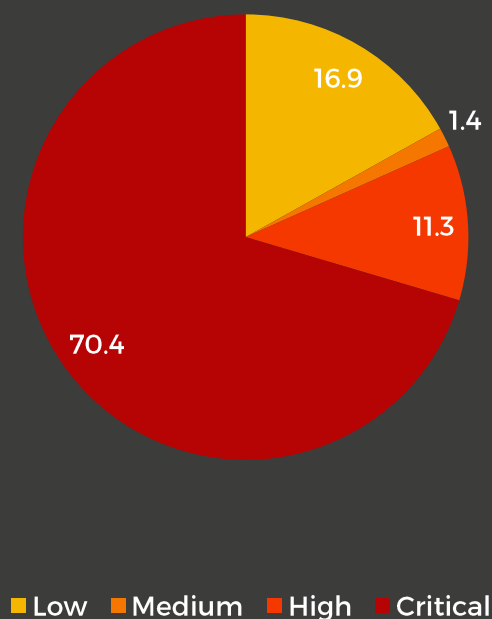
- *Desenhar a aplicação com base num modelo de acesso bem definido e de raiz, por exemplo role-based access control, de forma a minimizar inconsistências.*
- *Utilizar uma política de negar por omissão a não ser que a informação em causa seja pública.*
- *Forçar a que todos os pedidos passem pelo código de controlo de acessos.*
- *Manter o controlo de acessos server-side a sem recurso a informação proveniente do utilizador sem que esta seja devidamente validada.*
- *Não utilizar perfis hard-coded.*

SQL INJECTION

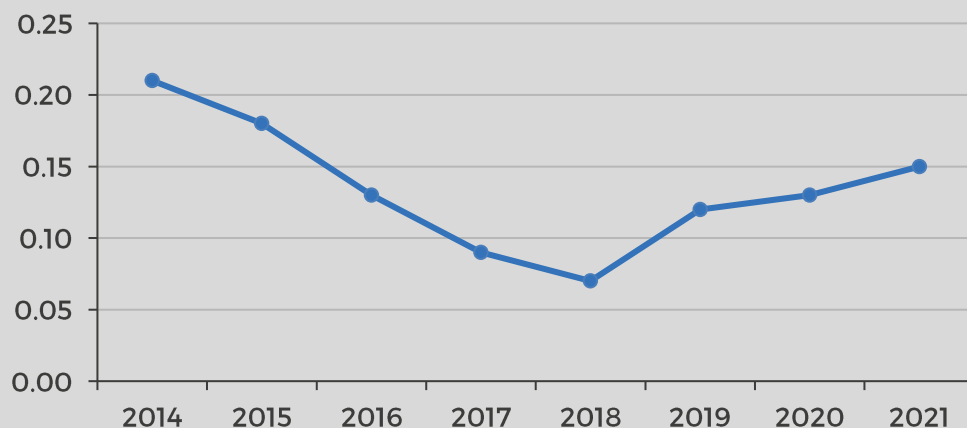
A vulnerabilidade **SQL Injection** tem um impacto significativo nas organizações, uma vez que permite a um atacante ter acesso a todos os conteúdos das bases de dados da aplicação, incluindo não só informação confidencial dos seus utilizadores, mas também credenciais de acesso. Isto significa que o seu impacto pode passar pelo acesso e leitura de conteúdos das bases de dados de forma indiscriminada, pela destruição de dados ou informação ou mesmo pelo controlo do servidor onde se encontra a tal base de dados.

No gráfico observa-se que é no setor dos Serviços onde é identificada uma quantidade mais significativa deste tipo de vulnerabilidade e que, apesar da tendência decrescente verificada de 2014 a 2018, tem-se observado desde então uma tendência crescente nas ocorrências de SQL Injection.

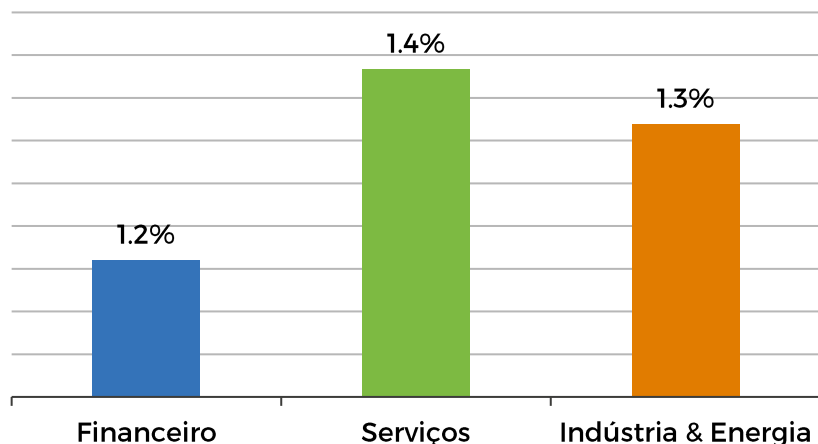
SQL INJECTION – SEVERIDADE



SQL Injection – Evolução



SQL INJECTION – SETOR



Nas tendências de SQL Injection para os diversos setores, destaca-se pela positiva o setor Financeiro, contrastando com o setor dos serviços em que se identificou mais vulnerabilidades de SQL Injection do que nos restantes setores. No entanto, com a introdução de frameworks de desenvolvimento, a quantidade de vulnerabilidades identificadas têm vindo a diminuir, apesar de nos últimos dois anos se notar uma tendência crescente. Este facto deve-se também à complexidade das aplicações aumentar e a necessidade de introdução de queries avançadas de forma manual, por parte dos developers, levando a que as proteções da framework não sejam implementadas.

Recomendações

- **Utilizar o Prepared Statements no código da aplicação:**
Os Prepared Statements permitem associar variáveis (input do utilizador) a dados a serem usados nas queries SQL, garantindo que os mesmos não podem alterar as condições ou a própria query SQL.
- **Filtrar e validar dados:**
Os dados oriundos de utilizadores, e sob o seu controlo, devem ser validados pela aplicação quanto ao seu conteúdo.
- **Rever o código:**
A revisão de código de forma a identificar potenciais erros de codificação que possam levar a falhas de segurança é de elevada importância. Consideramos que o código deve ser revisto por especialistas, os quais possam identificar estas potenciais falhas e permitir a correção das mesmas pelos programadores, antes da entrada em produção das aplicações.
- **Formar os programadores:**
De forma a aumentar o grau de segurança das aplicações, os programadores devem estar conscientes dos riscos associados aos erros de codificação das aplicações, bem como o potencial impacto na segurança da informação processada pelas mesmas, e dos servidores que as suportam. Através da formação adequada é possível reduzir o número de falhas de segurança existentes no código das aplicações, incrementando assim a resiliência das mesmas às falhas.

BROKEN AUTHENTICATION AND SESSION MANAGEMENT

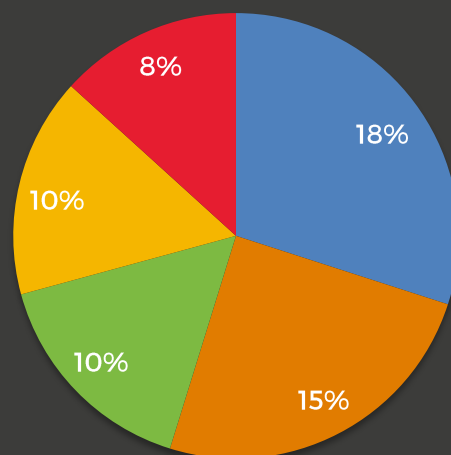
Autenticação é o processo que verifica se um utilizador é quem afirma ser e a gestão da sessão é o processo pelo qual o servidor mantém o estado das interações ativas com um determinado utilizador. É então fácil de entender que são componentes essenciais para que uma aplicação consiga interagir e distinguir os utilizadores e as vulnerabilidades identificadas neste contexto podem colocar em causa a informação sensível existente na aplicação.

Nos casos mais graves, estas vulnerabilidades podem permitir o acesso ilegítimo do atacante às aplicações e sistemas, com o intuito de assumir a identidade e privilégios do utilizador vítima do ataque. Este tipo de falha pode acontecer devido a eventuais falhas de configuração de controlos de segurança já incluídos de base nos sistemas.

No decorrer do ano de 2021 observou-se que cerca de 18% das vulnerabilidades de Broken Authentication and Session Management se referem às Cookies sem security flags, seguindo-se a enumeração de utilizadores com 15%, que se traduz na possibilidade de um atacante, na maioria das vezes de forma não autenticada, ter possibilidade de aferir a existência de determinado utilizador num sistema ou aplicação.

Com 10% temos as vulnerabilidades relacionadas com políticas de passwords fracas e a possibilidade de ataques de brute-force e, por fim, a utilização de HTTP Basic Authentication com 8%.

BROKEN AUTHENTICATION AND SESSION MANAGEMENT – SUBTIPO



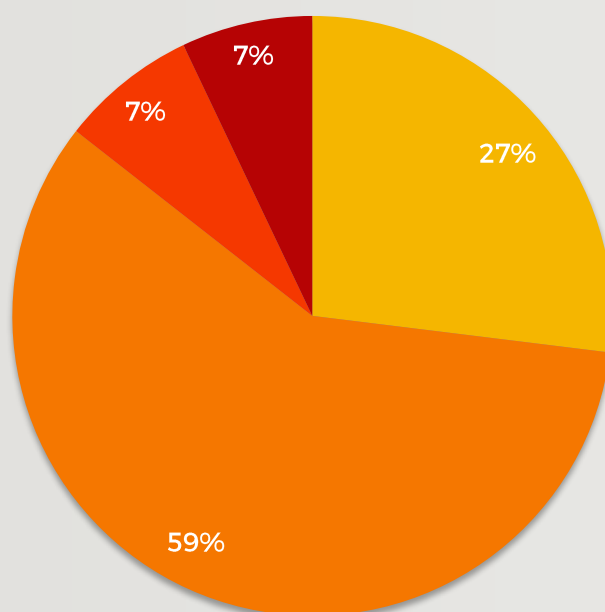
- Cookie Security Flags
- User Enumeration
- Weak Password Policy
- Brute-Force
- HTTP Basic Auth

É de salientar que, à exceção dos Cookies sem security flags, os restantes subtipos mais comuns deste tipo de vulnerabilidades (Weak Password Policy, User Enumeration, Brute-Force) podem ser combinados e levar assim ao comprometimento de contas de utilizadores, quando existentes em simultâneo no mesmo asset.

Tal como demonstrado no gráfico, as severidades no Broken Authentication and Session Management encontram-se distribuídas em todos os níveis, com maior incidência nas Medium, que registam 59%.

As Critical estão na ordem dos 7%, colocando em causa, de forma severa, a segurança dos sistemas e da informação.

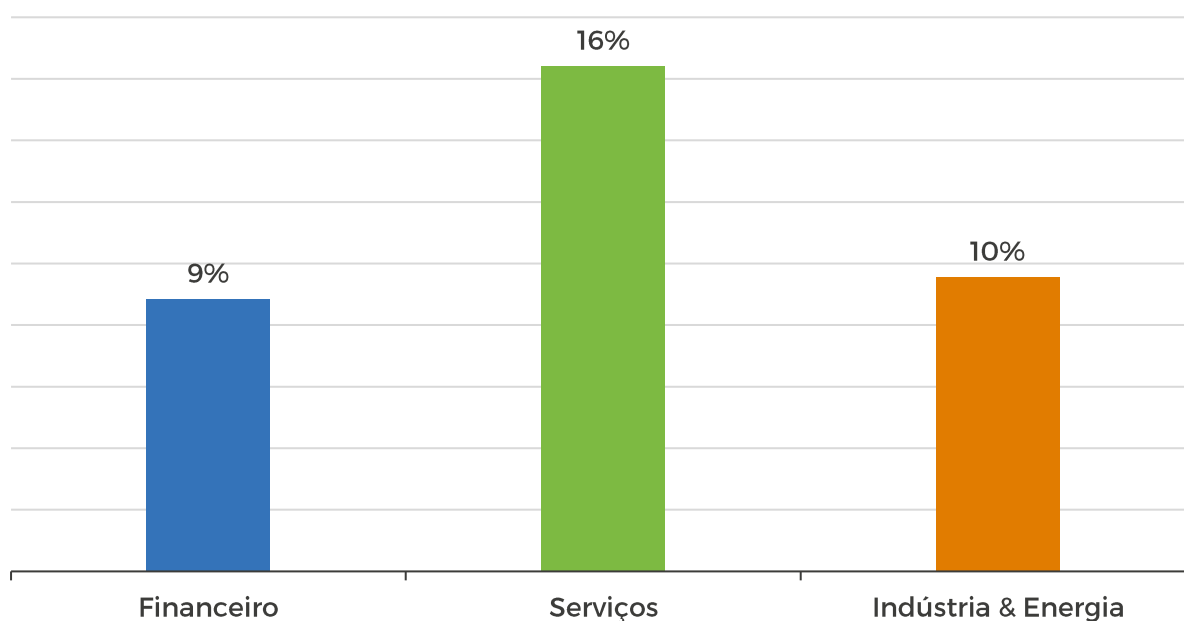
BROKEN AUTHENTICATION AND SESSION MANAGEMENT – SEVERIDADE



■ Low ■ Medium ■ High ■ Critical



BROKEN AUTHENTICATION AND SESSION MANAGEMENT – SETOR



Analisando o gráfico, o setor Financeiro destaca-se novamente pela positiva, com a menor percentagem de vulnerabilidades dentro desta categoria (9%). O setor dos Serviços é o que tem uma maior incidência, com 16% e o setor da Indústria & Energia com 10%. Novamente nesta categoria, a experiência das equipas técnicas, aliadas com a homogeneidade dos sistemas e aplicações têm um papel fundamental na prevenção deste tipo de vulnerabilidades.

Recomendações

- *Uso de two-factor-authentication para mitigar o uso de credenciais roubadas ou ataques de brute force.*
- *Uso de mecanismos de atraso na resposta ou bloqueio quando excedidas o número de tentativas de login definidas.*
- *Não fazer deployment de novos dispositivos sem alterar as credenciais por omissão.*
- *Não enviar credenciais por conexões não criptografadas.*
- *Manter boas políticas de passwords.*
- *Geração de um session ID Aleatório após o login bem sucedido.*
- *Implementação adequada de expiração de sessões (timeout).*

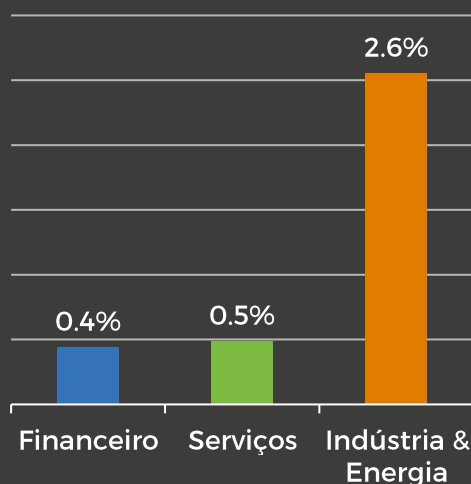
USING COMPONENTS WITH KNOWN VULNERABILITIES

Assumindo-se tipicamente como uma severidade crítica, o tipo de vulnerabilidade designado como Using Components with Known Vulnerabilities consiste na utilização de aplicações contendo vulnerabilidades conhecidas e grande parte das ocorrências (78%) significam a possibilidade de execução remota de código.

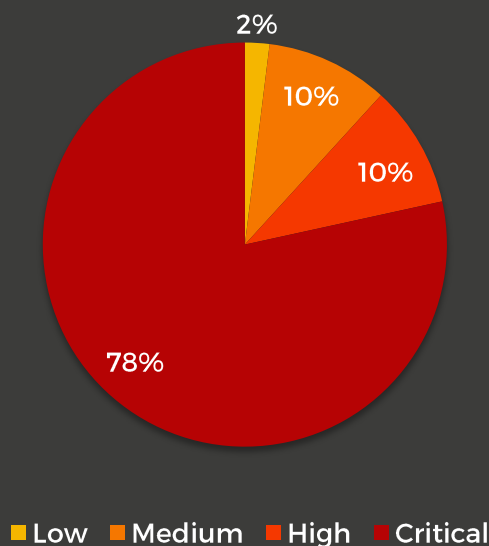
Olhando para o gráfico, conclui-se que o sector da Indústria & Energia é o grande impulsionador deste tipo de vulnerabilidade. Em organizações de grande dimensão, o processo de patching não é um processo simples, especialmente para equipamentos legacy onde por vezes não existem updates ou que os updates poderão comprometer, de alguma forma, o funcionamento dos mesmos. Deste modo, torna-se necessário otimizar os processos de gestão de patches e adicionalmente desenvolver capacidades para que, quando não é possível aplicar o patch, sejam identificadas medidas alternativas para a mitigação das vulnerabilidades.

Relativamente às vulnerabilidades críticas, a maioria das ocorrências em 2021, são originadas nas seguintes vulnerabilidades: CVE-2019-0708 (Bluekeep), CVE-2021-34527 (Windows Print Spooler), CVE-2021-44228 (Log4j).

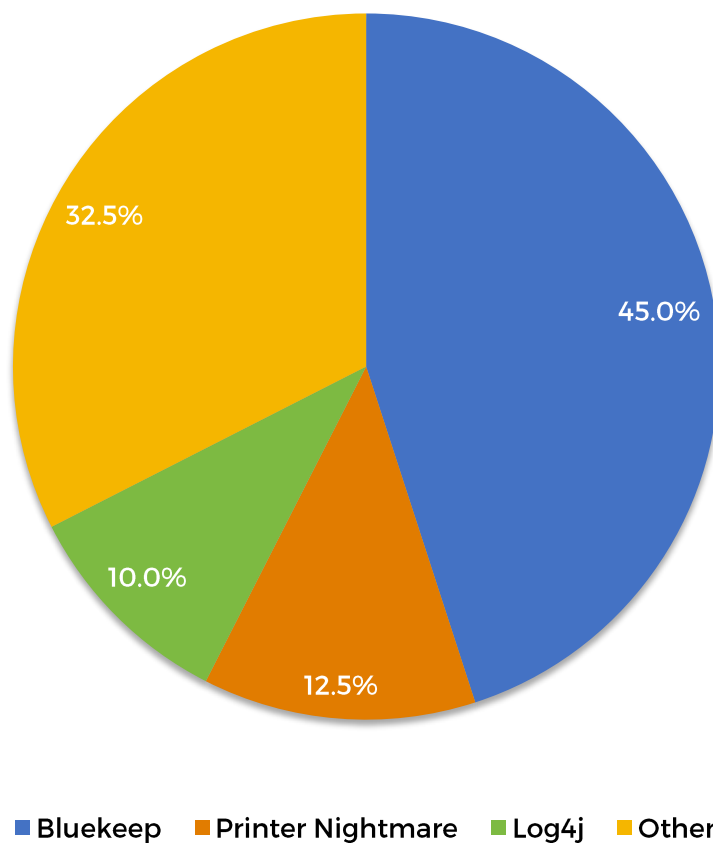
USING COMPONENTS WITH KNOWN VULNERABILITIES – SETOR



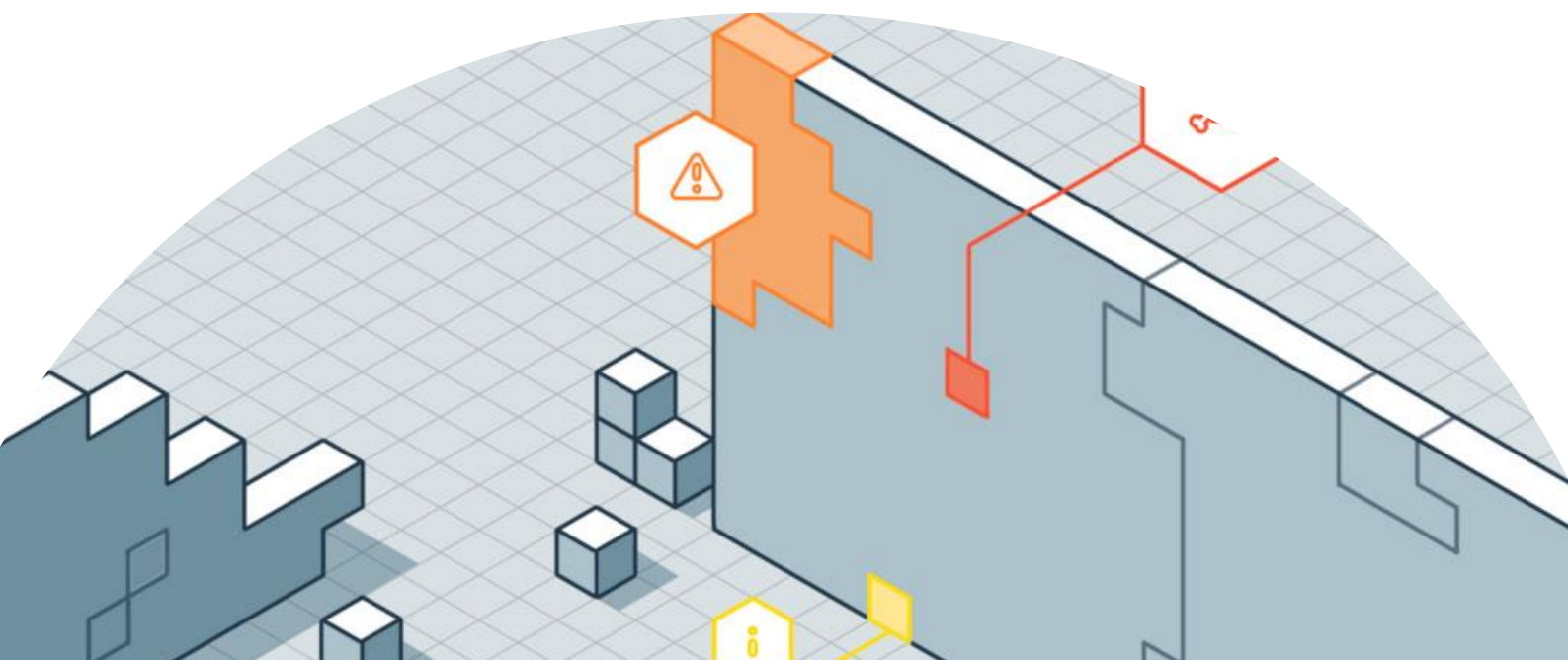
USING COMPONENTS WITH KNOWN VULNERABILITIES – SEVERIDADE

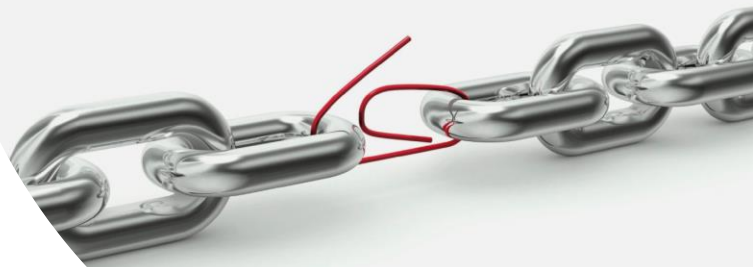


USING COMPONENTS WITH KNOWN VULNERABILITIES – SUBTIPO

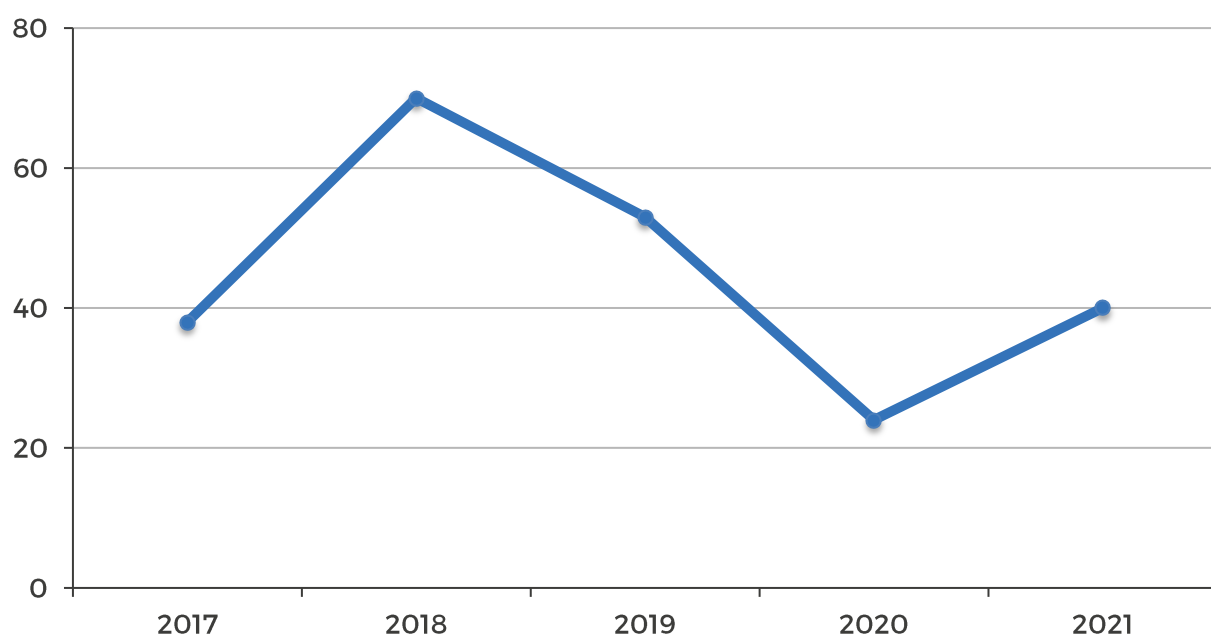


No entanto, considerando que a vulnerabilidade de Log4j apareceu em Dezembro de 2021 e o seu nível de risco elevado (permite execução de código remoto, de forma não autenticada e associado a uma utilização massiva do software vulnerável), vamos-nos debruçar um pouco mais sobre esta vulnerabilidade, e as medidas que a INTEGRITY tomou na proteção dos seus clientes.





Using Components With Known Vulnerabilities – Evolução



A análise de tendências revela que após um decréscimo acentuado de 2018 a 2020, existe um crescimento de 2020 para este ano, mas a percentagem de ocorrências continua com valores semelhantes a 2017.

Recomendações

- *Implementar um processo de gestão de ativos para inventariar as versões dos componentes tanto do lado do cliente como do servidor.*
- *Remover todas as dependências, funcionalidades, componentes, ficheiros, etc. que não sejam estritamente necessários ao funcionamento da aplicação/sistema.*
- *Apenas obter componentes a partir de fontes oficiais.*
- *Monitorizar por Software no fim de vida e considerar remover a aplicação ou implementar medidas de controlo de segurança alternativas.*

LOG4J

A 10 de Dezembro foi identificada uma vulnerabilidade que permitia a execução de código remoto (RCE), noLog4J, biblioteca de software utilizada por milhões de aplicações Java por todo o planeta. Esta vulnerabilidade a que foi atribuído o CVE-2021-44228 foi classificada com o CVSS de 10 (severidade máxima da base score).

A vulnerabilidade pode ser explorada através de um payload enviado às aplicações, por exemplo, através de parâmetros ou headers que uma vez passados ao Log4J são interpretados como um URL, que irá resultar no download de uma classe Java controlada pelo atacante e executar código com os privilégios da aplicação.

Apesar de apenas ter vindo a público a 10 de Dezembro, a vulnerabilidade de Log4j (Log4Shell) ainda contribuiu para as estatísticas anuais.

O destaque específico dado a esta vulnerabilidade, no contexto do presente documento, não é devido à quantidade de ocorrências, mas sim à sua severidade e à perceção pública relativa ao impacto que causaria, dado à sua existência quase onnipresente.

Na verdade, o número de vulnerabilidades de Log4J identificadas foi consideravelmente reduzido. Mesmo assim, as incidências identificadas, caso exploradas por um atacante teriam impactos desastrosos.

A abordagem da INTEGRITY na deteção da vulnerabilidade, foi baseada em 3 processos distintos:

- Scans automáticos com um plugin específico para o Log4j (scans automáticos).
- Script alterado internamente com pontos de injeção adicionais (scans semi-automáticos).
- Iteração manual para endereçar pontos de injeção incomuns e cobrir gradualmente todas as funcionalidades de cada aplicação (scans manuais).

No caso do Log4J ou vulnerabilidades de impacto semelhante, a rapidez e a utilização de diversos métodos de identificação e mitigação são essenciais para a compreensão e redução do risco e são também algo que as organizações devem executar internamente ou através de um parceiro de segurança da informação.

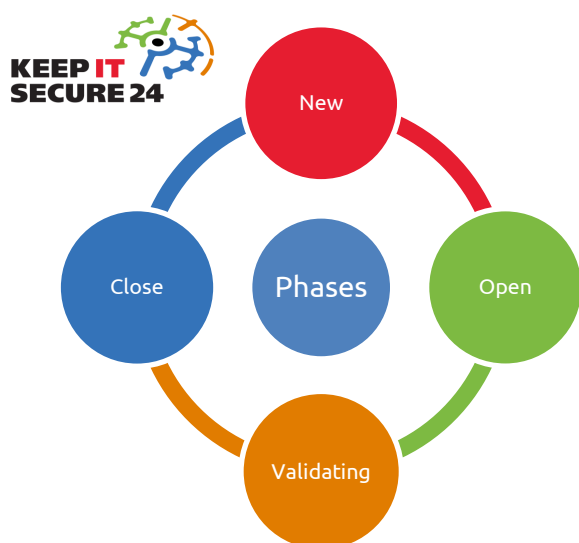


LOG4J

shift ↗

CICLO DE VIDA DAS VULNERABILIDADES

No contexto do KEEP-IT-SECURE-24, as vulnerabilidades passam por várias fases até que sejam consideradas resolvidas ou fechadas.



Tal como ilustrado na figura acima, o processo de resolução de vulnerabilidades compõe-se por várias fases:

- **New:** identificação e publicação na plataforma KEEP-IT-SECURE-24;
- **Open:** abertura para análise da vulnerabilidade por parte do cliente;
- **Validating:** validação do sucesso da correção da vulnerabilidade;
- **Close:** quando está resolvida.

No entanto, antes de entrar neste último estado, o close, pode haver uma reabertura ou não, havendo aqui duas possibilidades:

- A INTEGRITY conclui que a implementação dos controlos foi efetivamente bem feita, e para a fase Close.
ou
- A INTEGRITY conclui que, por alguma razão, o cliente não implementou bem os controlos, o que significa que ainda há riscos, e passa então da fase Validating para a fase Open.

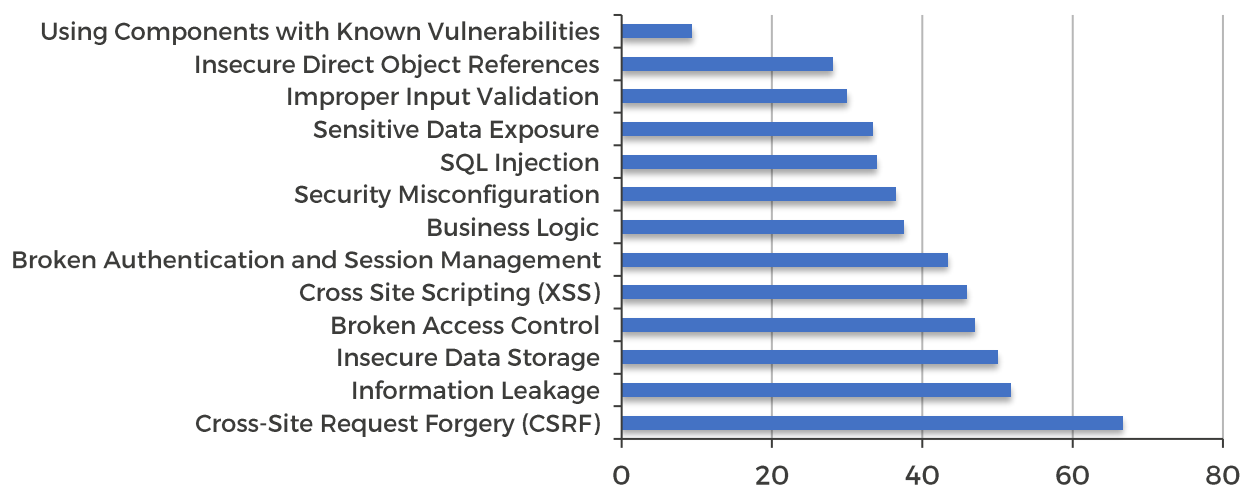
De forma a melhorar os processos de resolução de vulnerabilidades, deve olhar-se e fazer uma análise às dificuldades de fecho associadas a determinadas vulnerabilidades. Há que perceber o número de vezes que determinada vulnerabilidade foi considerada “resolvida” pelo cliente e que, após reavaliação por parte da INTEGRITY, foi reaberta por não estar totalmente resolvida.



DIFICULDADES DE RESOLUÇÃO EFETIVA

TIPOS DE VULNERABILIDADES QUE REGISTRARAM MAIS REABERTURAS EM 2021

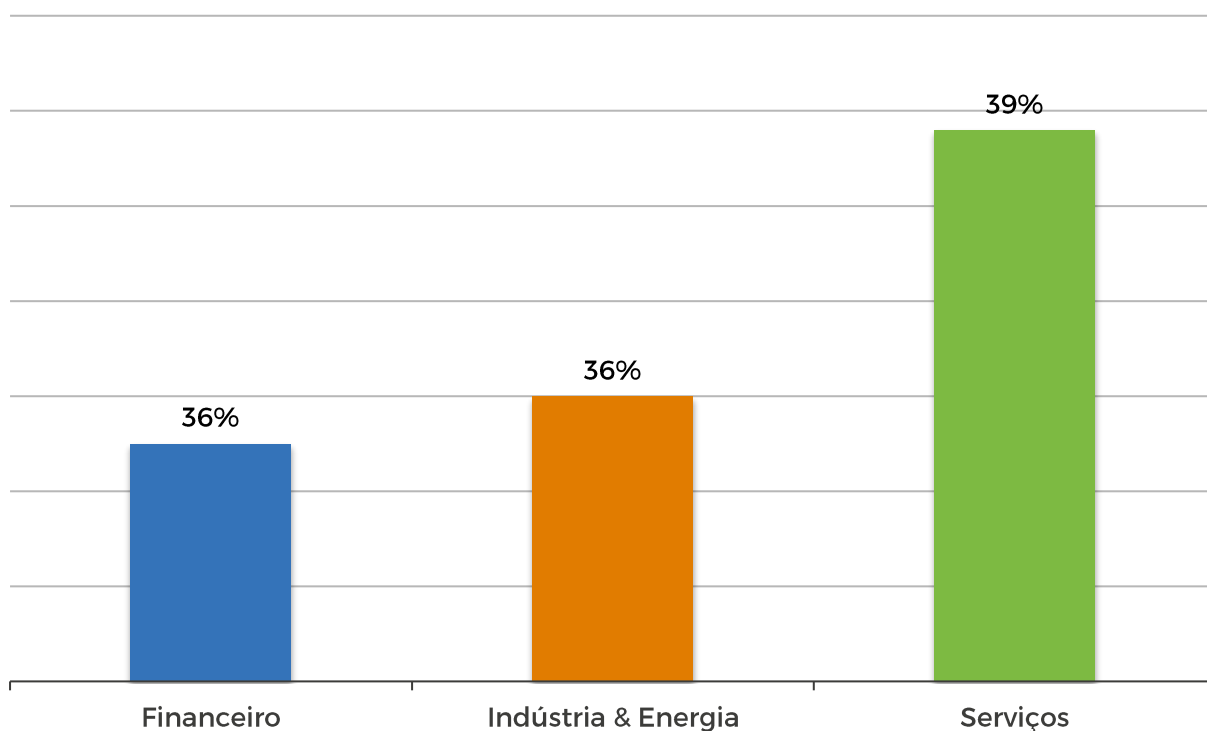
Percentagem de vulnerabilidades que não foram resolvidas à primeira tentativa em 2021 para os tipos mais comuns.



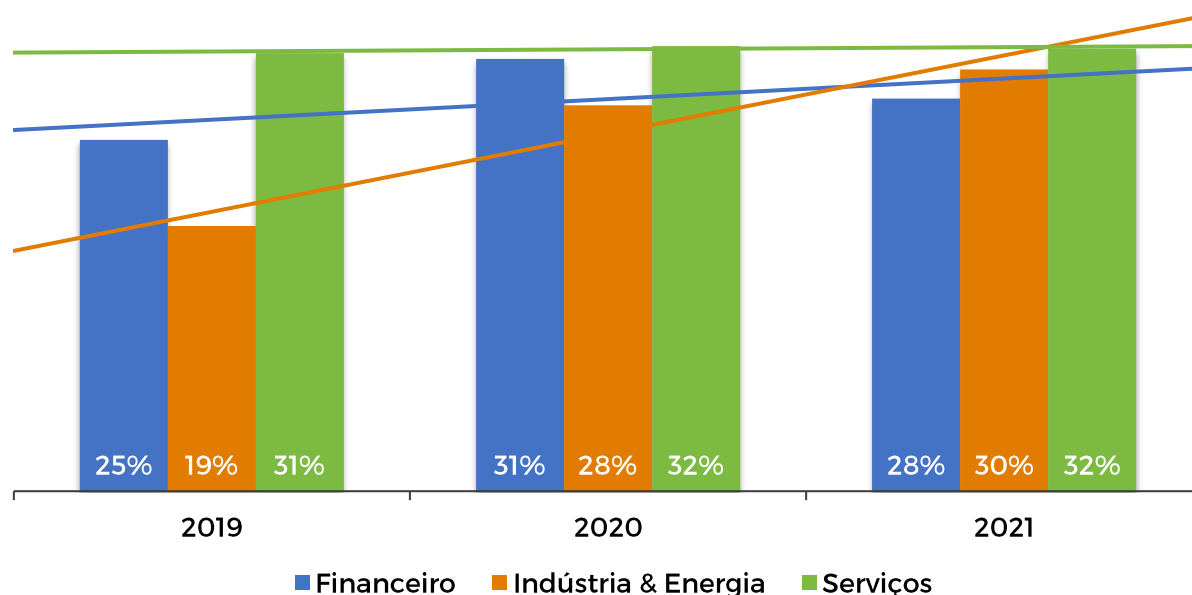
O gráfico mostra-nos que para os tipos de vulnerabilidades mais comuns em 2021 foram reabertas entre 30% a 50%, cifrando-se a média em 37,2%. Porém, podemos observar alguns tipos de vulnerabilidades que divergem destes valores e se destacam. São eles o CSRF e Using Components With Known Vulnerabilities, sendo o primeiro aquele com maior quantidade de vulnerabilidades reabertas e o último com menor. Este posicionamento na escala, faz perfeito sentido, já que a ausência de CSRF token implica desenvolvimento relevante na aplicação web e a existência de vulnerabilidades do tipo Using Components With Known Vulnerabilities surge normalmente quando foi descurada a aplicação de um patch ou versão atual de software, o que normalmente é efetuado com relativa facilidade.

PERCENTAGEM DE VULNERABILIDADES REABERTAS POR SETOR

Relativamente à capacidade de fecho de vulnerabilidades à 1ª tentativa, constata-se através do gráfico abaixo que em 2021 os 3 setores analisados estiveram mais ou menos equiparados, com o setor Financeiro a registar resposta ligeiramente melhor à resolução das vulnerabilidades, com menos vulnerabilidades reabertas, enquanto o setor dos Serviços é o setor com maior número de vulnerabilidades reabertas.



EVOLUÇÃO POR SETOR, DO FECHO VULNERABILIDADES FACE ÀS PUBLICADAS



Em relação à evolução de fecho de vulnerabilidades observa-se que em 2021 foi o setor dos Serviços que teve maior capacidade de resposta, com 32% de vulnerabilidades fechadas com sucesso. Porém, ao observar o gráfico anterior, de percentagem de vulnerabilidades reabertas, verificamos que o sector dos serviços é o menos assertivo no fecho das vulnerabilidades.

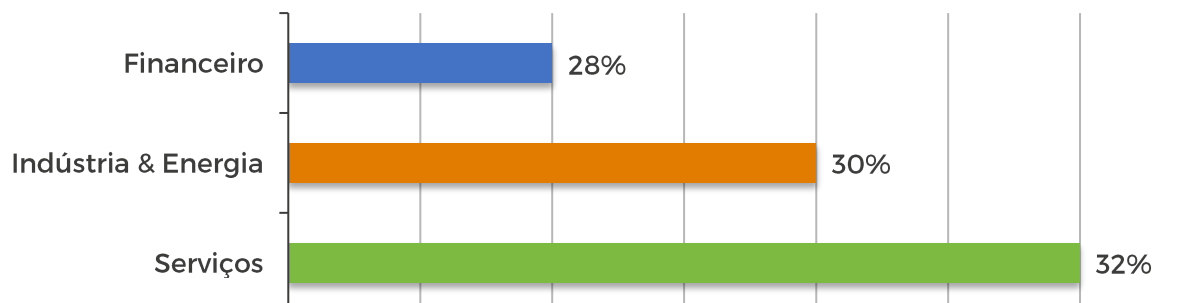
No ano de 2021, o setor da Indústria & Energia conseguiu fechar 30% das vulnerabilidades e o setor Financeiro foi o que menos vulnerabilidades fechou com 28% de vulnerabilidades corrigidas face às publicadas.

Fica patente no gráfico uma tendência de crescimento da percentagem de vulnerabilidades fechadas face às

publicadas para os sectores Financeiro e Indústria & Energia, demonstrando cada vez maior relevância da segurança nas organizações, tornando-se um pilar fundamental de suporte ao desenvolvimento.

A tendência de crescimento da percentagem de vulnerabilidades fechadas não se regista no setor dos Serviços, provavelmente devido a uma maior dinâmica na entrada de novos clientes, levando a uma diluição dos benefícios inerentes à utilização de um serviço de testes continuados, como é o caso do KEEP-IT-SECURE-24. Deste modo, a experiência e o treino obtido pelas equipas de segurança dos clientes experientes com o serviço, não fica evidenciado nos gráficos históricos.

PERCENTAGEM DE VULNERABILIDADES FECHADAS POR SETOR



Tal como demonstrado no gráfico abaixo, no top 5 dos tipos de vulnerabilidades mais resolvidas em 2021 estão as 4 vulnerabilidades mais comuns: Sensitive Data Exposure (28%) e Security Misconfiguration (22%), seguindo-se o Broken Authentication and Session Management (12%), o Cross Site Scripting (12%) e, por último, a categoria de Insecure Direct Object References (6%).

Este resultado encontra-se correlacionado com a dificuldade da implementação de correções, refletida no gráfico de Reaberturas por tipo de vulnerabilidades.

Conforme vimos nas descrições acima, grande parte das vulnerabilidades de Sensitive Data Exposure, são relacionadas a cifras fracas ou problemas com certificados. A correção destas vulnerabilidades é, na maioria dos casos, trivial.

De igual modo, o Security Misconfiguration contém um grande número de falta de Security Headers e de visualização de Stack Traces, também vulnerabilidades de fácil resolução.

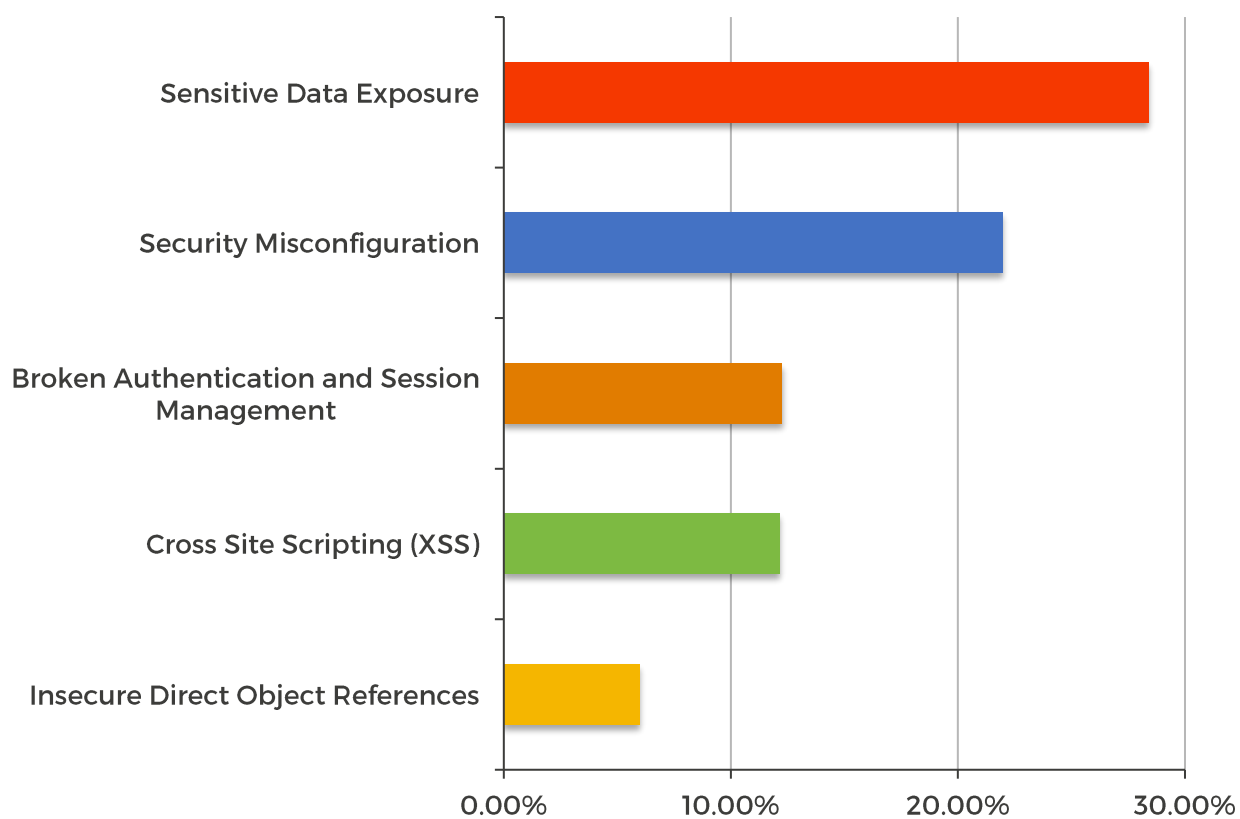
Nas 2 categorias seguintes, começa a aumentar a complexidade de resolução, como a implementação de autenticação de 2 fatores (2FA) ou introdução de mecanismos de controlo para protecção dos identificadores de sessão, no caso de Broken Authentication and Session Management, ou a codificação de inputs de utilizador numa perspetiva geral da aplicação, no caso de Cross Site Scripting.

Por último, no caso de Insecure Direct Object References, este requer a validação de permissões da aplicação e pode exigir uma mudança na lógica de funcionamento de diversas funcionalidades da aplicação, modificando identificadores iteráveis por identificadores aleatórios como GUIDs.





VULNERABILIDADES MAIS CORRIGIDAS EM 2021

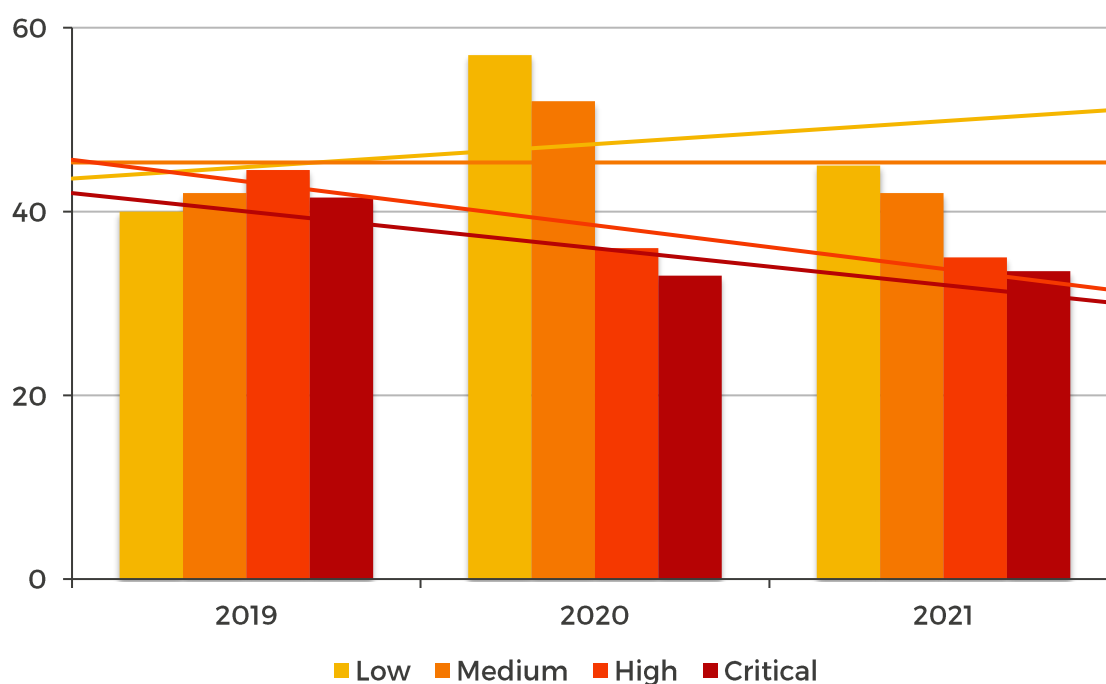


TEMPOS DE VIDA

TEMPO DE VIDA PARA AS 5 VULNERABILIDADES MAIS RESOLVIDAS EM 2021

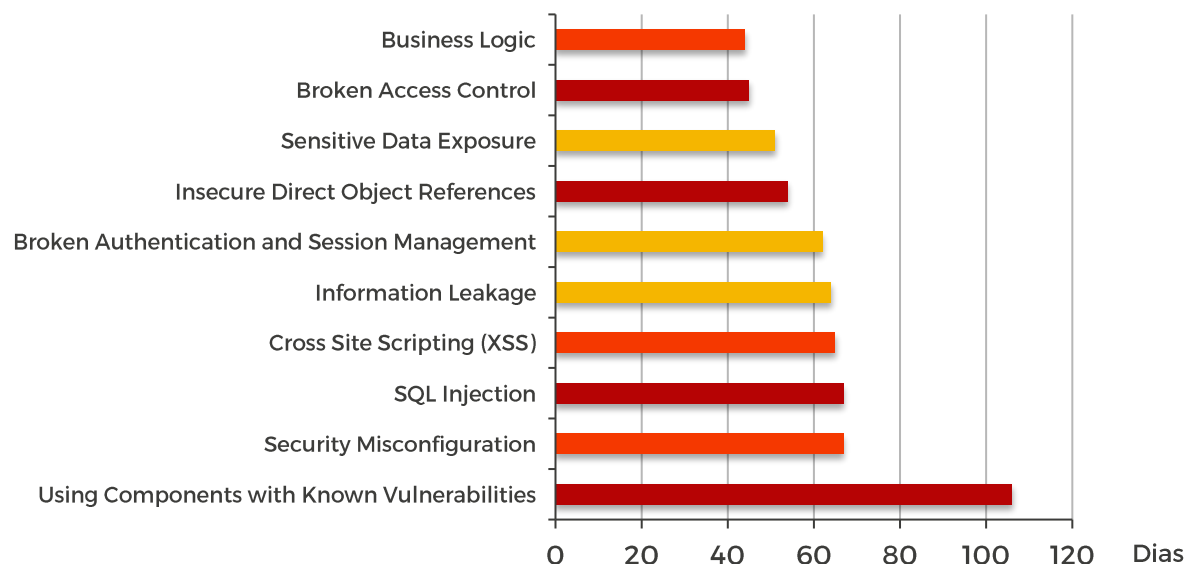
O tempo de vida da vulnerabilidade corresponde à janela temporal entre o momento de identificação e publicação no portal KEEP-IT-SECURE-24 da mesma até ao momento em que se encontra comprovadamente resolvida.

TEMPOS DE VIDA POR SEVERIDADE



Ao analisar os tempos de vida das vulnerabilidades por severidade, é com satisfação que verificamos uma tendência de descida do tempo de vida das vulnerabilidades críticas e altas. Verifica-se também uma tendência de estabilização do tempo de vida das vulnerabilidades médias e um aumento das baixas.

MÉDIA DE TEMPOS DE VIDA PARA AS 10 VULNERABILIDADES MAIS RESOLVIDAS EM 2021



Através deste gráfico pode-se constatar que o tempo de vida é mais longo para as vulnerabilidades publicamente conhecidas em produtos off-the-shelf cujo patch de segurança já existe - Using Components With Known Vulnerabilities. Esta conclusão parece contrariar a intuição, já que o patch existe e não é aplicado após a publicação da vulnerabilidade. Nestes casos a lentidão na resolução poderá estar relacionada com o facto de se tratarem de sistemas que não se encontram expostos e cuja aplicação de patching gera algum receio de impactos adversos.

No extremo oposto, com menos tempo de resolução observamos as falhas de business logic que apesar de na sua média serem de severidade High do ponto de vista técnico, poderão ser

percepcionadas como mais impactantes do ponto de vista de negócio, desencadeando assim um sentido de urgência acentuado.

O gráfico permite-nos observar que não existe uma relação entre a severidade das vulnerabilidades e o seu tempo de vida.

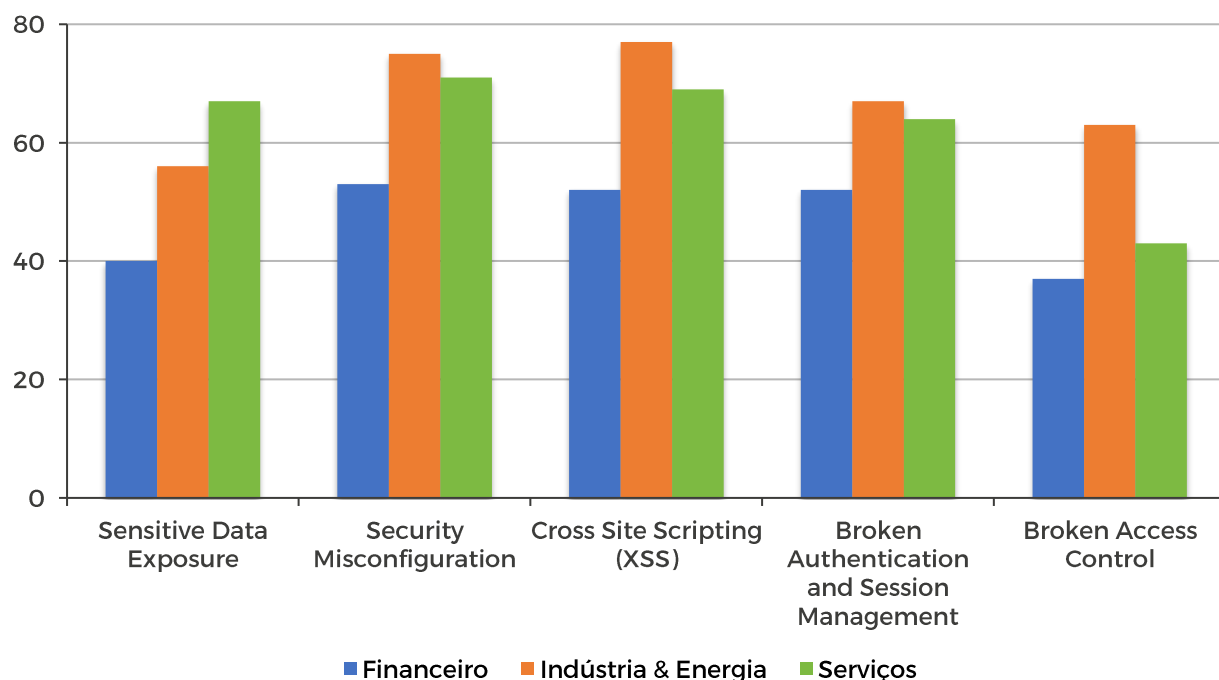
Podemos também observar que, ao contrário do esperado, também não se verifica uma relação entre quantidade de incidências fechadas (Vulnerabilidades mais fechadas de 2021) e tempo de vida das vulnerabilidades. Esta observação permite-nos constatar que existe ainda algum espaço de melhoria para a otimização dos tempos de vida, com o fecho do mesmo tipo de vulnerabilidade repetidamente.







TOP 5 TEMPOS DE VIDA POR SETOR

O gráfico abaixo aponta o setor Financeiro como aquele que, de forma transversal, é o mais rápido a fechar vulnerabilidades, seguindo-se os Serviços e a Indústria & Energia.

Este padrão segue as observações anteriores com o setor Financeiro a ter uma maior performance, provavelmente devido a uma maior maturidade dos processos de gestão de segurança. O setor da Indústria & Energia é o setor que demora mais tempo a fechar vulnerabilidades, devido à complexidade dos seus sistemas e potencial impacto na implementação de correções.



Median of days to close		2017	2018	2019	2020	2021	
	Critical	20	31	41,5	33	33,5	↑
	High	28,5	49	44,5	36	35	↓
	Medium	39	56	42	52	42	↓
	Low	34	49	40	57	45	↓

Mediana relativamente ao fecho por severidade.

Apesar de um ligeiro aumento de meio dia do tempo de resolução das vulnerabilidades críticas, é com agrado que observamos uma tendência global decrescente nos tempos de resolução. A contribuir para este fator temos por um lado, um aumento da importância atribuída à segurança, com todos os casos mediáticos de ataques informáticos, levando as organizações a aumentar os recursos disponíveis para proteger a sua informação e infra-estruturas de suporte. Por outro lado, a execução de pentests regulares, proporciona uma otimização dos processos internos das organizações e a aprendizagem das equipas alocadas à resolução das vulnerabilidades, tornando-se ao longo do tempo mais eficientes a mitigar as vulnerabilidades identificadas nos seus sistemas e em alguns casos a prevenir o aparecimento de novas.



CONCLUSÃO

TOP VULNERABILIDADES E RECOMENDAÇÕES

Nos dias de hoje, investir em **Cibersegurança** é uma questão absolutamente prioritária.

É esta a mensagem que, de forma rápida e direta, urge passar após ler e analisar os dados apresentados neste relatório, que acaba por ser um espelho dos desafios, vicissitudes e conquistas que ao longo de 365 dias as empresas de três setores de atividade económica importantes do mercado nacional e internacional passaram, face à realidade das incidências de Cibersegurança.

Sector Financeiro, sector da Indústria & Energia e sector dos Serviços, foi sobre estas áreas que incidiu a análise feita, tendo ficado claro que se encontram todos nivelados em relação às práticas de cibersegurança.

A contagem reduzida de vulnerabilidades de severidade Crítica e High face ao total de vulnerabilidades, é uma métrica que a nosso ver tende a refletir, uma escolha assertiva de soluções, implementação adequada de controlos de segurança e boas práticas de desenvolvimento. De uma forma geral vemos esta métrica com tendência a decrescer de ano para ano em todos os setores, no entanto, o sector dos Serviços destacou-se pela menor percentagem de vulnerabilidades críticas identificadas face ao ano anterior, contribuindo assim para o decréscimo global de vulnerabilidades desta severidade em 5%. Ficou também evidente pela análise efetuada que, no que concerne às vulnerabilidades de severidade High, o decréscimo geral de 9% registado face ao ano passado, já teve contribuição de todos os setores.

A reabertura de vulnerabilidades é uma métrica reveladora face à eficácia dos processos implementados pelas organizações e capacidade de melhoria contínua. Nesta vertente pudemos observar que o sector Financeiro foi aquele que mostrou maior assertividade com menor quantidade de reaberturas de vulnerabilidades.

A análise dos tempos de vida das vulnerabilidades permitiu-nos observar que a eficiência nos processos de fecho anda a par com a eficácia de fecho já que o sector Financeiro destacou-se também consistentemente nesta vertente, com maior rapidez na resolução de vulnerabilidades. A eficiência de fecho demonstrada pelo sector Financeiro é transversal e regista-se também individualmente para a maioria dos tipos mais comuns de vulnerabilidades.



Apesar de na globalidade os setores se apresentarem nivelados, é de relevar a maior performance do setor Financeiro na capacidade de agir sobre as vulnerabilidades identificadas com maior rapidez e assertividade. Esta observação poderá estar relacionada com uma maior maturidade, dado que historicamente, é um dos setores que mais cedo foi alvo de ataques e dedicou atenção ao tema da segurança da informação.

É interessante verificar, de forma transversal, que o aumento acentuado de exposição de serviços online que se tem verificado nos últimos anos não se refletiu no aumento da percentagem de vulnerabilidades de severidade High ou Critical, o que nos parece deixar evidente que a segurança é um tema muito presente na tomada de decisão nas organizações avaliadas.

A análise dos dados por setor permitiu observar que o setor Financeiro apresenta uma maior incidência de utilização de cifras consideradas fracas, ainda assim cuja exploração é bastante improvável, provavelmente para garantir melhor compatibilidade aos seus clientes na interação com os serviços online.

O setor dos Serviços parece ser o que apresenta maior heterogeneidade de aplicações, registando também uma tendência para aplicações incrementalmente mais complexas, cuja operação e manutenção vai requerendo acompanhamento, por parte das equipas técnicas. Este facto fica refletido em maior percentagem de vulnerabilidades do tipo Security Misconfiguration.

Podemos concluir ainda que, para cada setor, existe uma maior incidência para certas categorias de vulnerabilidades, inerentes à composição dos seus sistemas, aplicações e métodos de atuação.

Por mais que já tenhamos referido este ponto, não há como não voltar a mencioná-lo: a pandemia veio alterar o mercado e acelerar o processo de Transformação Digital de grande parte do tecido empresarial, trazendo por um lado aspetos positivos, mas favorecendo, por outro e de forma inevitável, as atividades ilícitas online e os ataques.

São muitas as pessoas que trabalham agora a partir de casa, sendo prioritário garantir a confidencialidade, integridade e disponibilidade da informação que deixou de estar restrita aos sistemas das empresas, encontrando-se mais exposta e vulnerável.

A pandemia evidenciou a utilidade de avaliação e ação da segurança da informação em três eixos: tecnologia, pessoas e processos, os quais são absolutamente imprescindíveis para qualquer organização e cuja simbiose se traduz numa clara vantagem competitiva. Vivemos tempos incertos, onde tudo é rápido, até mesmo a velocidade a que se desenvolvem novas estratégias de ataque, exigindo por isso também rapidez na resposta dada, ou seja, na ação e na prevenção.

Neste contexto, as empresas que desenvolvem e implementam estas soluções de prevenção e recuperação dos sistemas, como a INTEGRITY part of Devoteam, têm de estar sempre um passo à frente e em constante estado de alerta.

O risco é algo que tem de ser gerido e as empresas têm de ter noção das ameaças a que diariamente estão expostas. Há cada vez mais ataques cibernéticos reportados e, infelizmente, os atacantes parecem estar mais sofisticados e criativos do que nunca. As empresas têm, por isso, de agir e implementar medidas de combate face a este problema. No entanto, isto é algo que deve ser feito de forma contínua e encarado como uma prática e um processo para ficar e não, como algo pontual.

Presente há 13 anos no mercado e com uma equipa altamente experiente e qualificada, a INTEGRITY part of Devoteam tem vindo a auxiliar os clientes a identificar potenciais riscos, nomeadamente vulnerabilidades técnicas através dos Testes de Intrusão Pontuais ou Persistentes - **KEEP-IT-SECURE-24** - providenciando recomendações e um apoio ímpar para a mitigação dos problemas identificados.





Há que realçar que, neste momento, as organizações estão cada vez mais preocupadas com o tema da resiliência, o qual está aliás a marcar uma tendência no mercado. E quando falamos neste conceito de resiliência, falamos de capacidade de superação, adaptação, agilidade diante de dificuldades ou situações adversas consideradas um risco. E, numa altura em que estamos todos - organizações e mercado - focados nesta temática, é fundamental ter à disponibilidade uma tecnologia de Testes Persistentes.

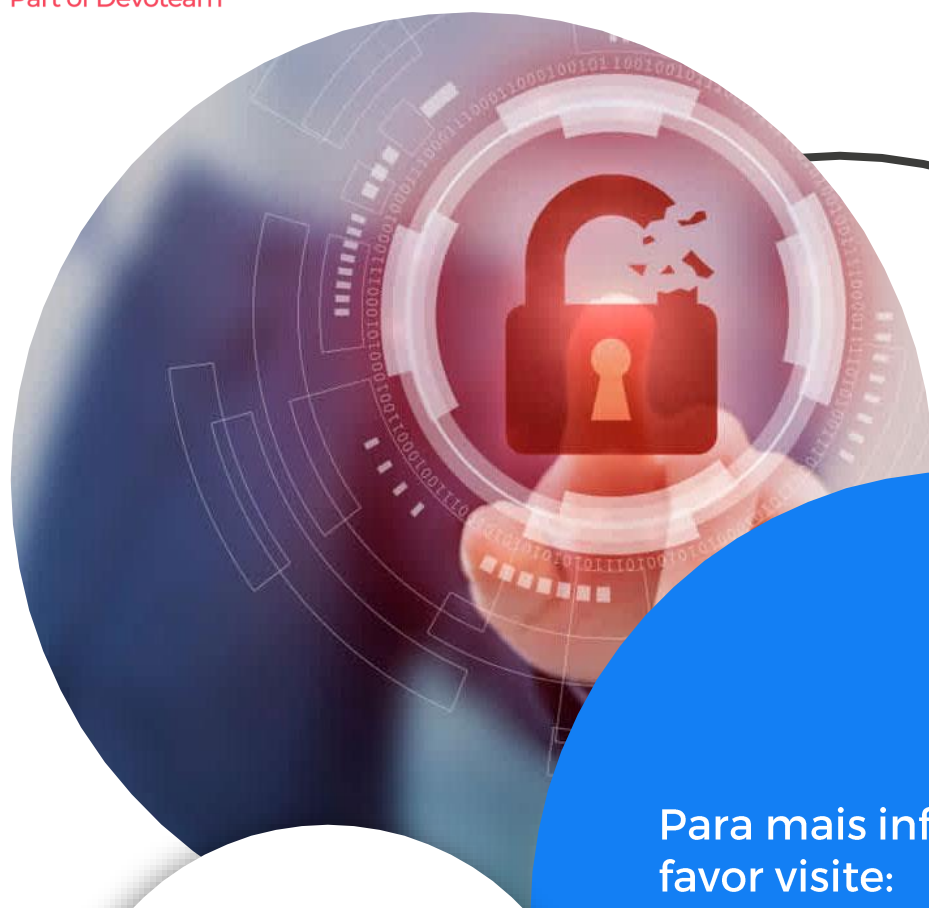
Focando outro ponto também importante - **os comportamentos das pessoas** - tem-se notado uma consciência cada vez maior em relação aos riscos, impactos e consequentemente da urgência em apostar em soluções para fazer frente a este tipo de ameaças. No entanto, é necessário continuar a investir nesta sensibilização e educação junto de cada um, para a adoção de atitudes e comportamentos mais adequados. Transformar esta sensibilização em medidas concretas é um caminho.

O tema da Segurança da Informação deverá estar no topo das prioridades de qualquer gestor e esta mensagem deveria ser sempre passada a toda a empresa, até porque está comprovado que os colaboradores continuam a ser os pontos mais vulneráveis. É fundamental por isso, investir nas pessoas, para que fiquem devidamente formadas e alertadas para os riscos de certos procedimentos que tomam.

As **recomendações** são igualmente um item a reter, consistindo num conjunto de boas práticas e orientações que todos devemos seguir para maximizar os níveis de cibersegurança. Há as mais conhecidas e básicas, como o reportar e-mails suspeitos ou manter boas políticas de passwords, mas há outro patamar: ao nível das SSL/TLS deve-se definir “checklists” de configuração, assim como garantir a desabilitação de protocolos obsoletos ou pouco seguros; fazer updates, que consistem na verificação regular e atenta das atualizações, e caso haja vulnerabilidades Critical, devem ser implementados processos de atualização rápida.

Os gráficos neste documento são elucidativos: as ameaças estão em constante crescimento e, de ano para ano, aparecem novas formas de ataque. Olhar para estes números e percentagens deve servir para nos mostrar a importância de rever e reinventar dinâmicas e rotinas, de forma a proteger o ativo de maior valor de qualquer negócio: os dados e a informação.

Pelo seu valor estratégico incalculável, é imperativo planear e estabelecer uma estratégia virada para a **Segurança da Informação**.



Para mais informações, por favor visite:

- www.integrity.pt
- www.keepitsecure24.com



PORTUGAL

Edifício Atrium Saldanha
Praça Duque de Saldanha, nº 1,
2º andar
1050-094, Lisboa | Portugal
T: +351 21 33 03 740
E: info@integrity.pt

UNITED KINGDOM

43 Berkeley Square
Mayfair, Westminster
London, W1J 5FJ | U.K.

ESPAÑA

Calle Cronos 63, 4ª planta
Oficina 2
28037, Madrid | España
T: +34 91 376 88 20

