Overview 2020

Top Vulnerabilidades e Recomendações

maio 2021

KEEP IT SECURE 24

INTEGRITY
Part of Devoteam

Índice

A **INTEGRITY** é uma empresa portuguesa que atua e fornece serviços especializados e inovadores de Segurança da Informação nas áreas de Auditoria e Consultoria. É certificada em ISO 27001 e ISO 9001, certificada pelo PCI e membro CREST e do CIS – Center for Internet Security. Conta com uma experiência de 12 anos, e opera em mais de 19 países nos cinco continentes, graças ao fornecimento de serviços de valor acrescentado em Cibersegurança, que combinam a sua experiência 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, ISO 27001, PCI-DSS e soluções de gestão de risco a terceiros, suportadas pelas suas plataformas - IntegrityGRC e VulnManager.

Introdução

Top Vulnerabilidades e Recomendações

Serve o presente relatório para apresentar os últimos dados referentes às vulnerabilidades detetadas no âmbito do serviço de KEEP-IT-SECURE-24 para clientes, nacionais e internacionais, da INTEGRITY em 2020 e respetivas recomendações para as evitar.
Importa frisar que os dados em questão foram recolhidos e tratados de forma anónima, tendo havido o cuidado de excluir os outliers por se diferenciarem drasticamente de todos os outros, sob pena de enviesarem os resultados e a análise feita.

Neste documento é feita uma análise objetiva, mas não menos minuciosa das incidências de cibersegurança, o seu nível de severidade, a sua evolução e natureza, com especial enfoque em três grandes setores de atividade económica: o Setor Financeiro (um setor maduro e pioneiro a atuar nesta matéria), o Setor da Indústria & Energia e o Setor dos Serviços. Por fim, como não poderia deixar de ser, são alinhadas recomendações para a mitigação das principais questões e problemas identificados.

Falar do ano 2020 é falar de um dos anos mais desafiantes e imprevisíveis de que há memória – devido ao COVID-19 - no qual todas as pessoas foram postas à prova, tornando-se (em tom otimista) mais resilientes e fortes do que nunca. Equipas inteiras de colaboradores viram-se obrigadas a trabalhar a partir de casa, independentemente do grau de preparação das empresas que num ápice tiveram de se reinventar e muitas delas dar, finalmente, o tal passo tecnológico absolutamente fundamental, mas consequentemente adiado por razões várias.
Foi, e continua a ser, um enorme desafio para as empresas conseguirem dar continuidade de negócio, tendo os colaboradores fora dos espaços de trabalho. Isto exigiu todo um reinventar de procedimentos e normas, toda uma adaptação a uma nova realidade para a qual ninguém teve tempo de preparação.

O teletrabalho é o novo normal e, se por um lado, os colaboradores deverão ter em conta que deixaram de trabalhar num ambiente de certa forma “protegido e controlado”, por outro as organizações têm de se consciencializar que ficaram mais expostas, continuando a ser prioritária a questão da segurança do seu principal ativo: a informação.

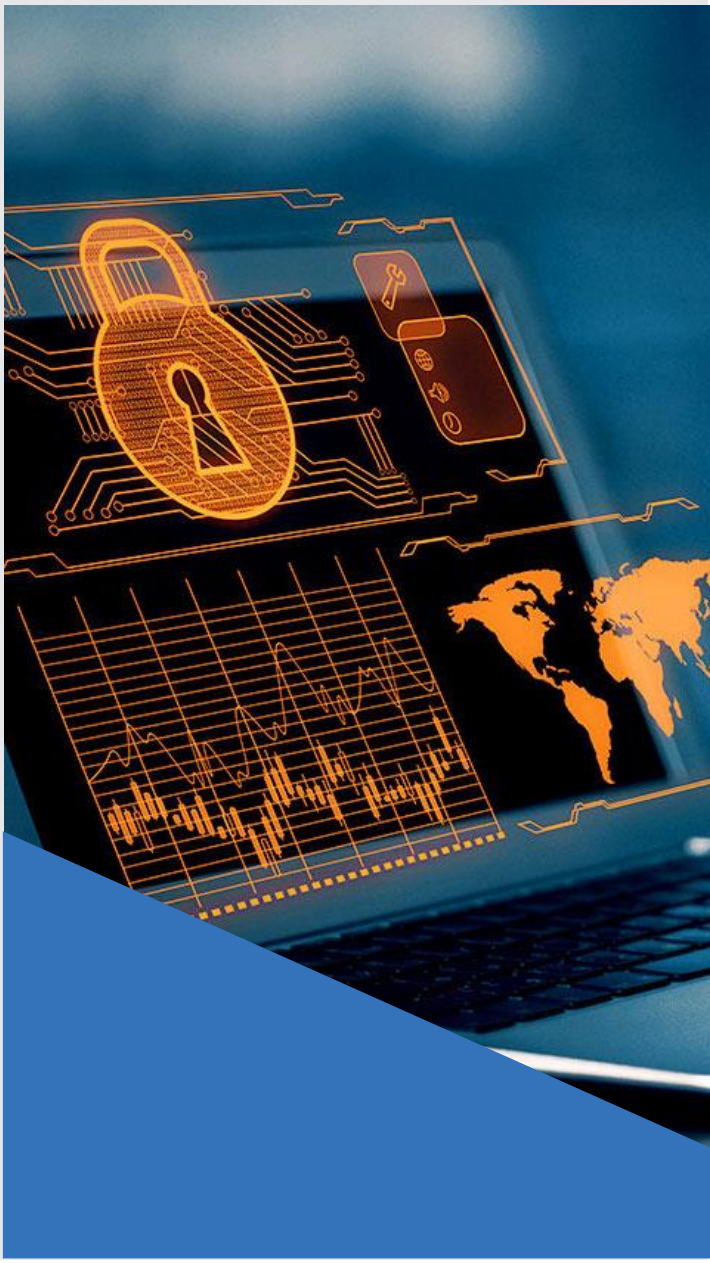
Dados oriundos da ANACOM, mostram um aumento de 61,1% no consumo do serviço de Internet fixa, no primeiro semestre de 2020, comparado com o mesmo semestre do ano anterior, aumento este que poderá estar relacionado com as mudanças acima referidas na organização do trabalho, fruto das medidas de combate à pandemia. Estas medidas promoveram não só o trabalho e a aprendizagem à distância, mas também a tendência para o isolamento dos indivíduos, uma maior dependência em relação aos serviços digitais e um uso mais frequente de computadores portáteis e dispositivos móveis.

É impossível não referir também os desafios e o potencial transformador da Internet of Things (IoT) que, se por um lado promete mais rapidez e eficiência, por outro aumenta a exposição e o risco.

Os riscos aos quais as organizações estão expostas são diversos, variando desde quebras de confidencialidade até à negação de serviços, aplicação de multas e questões de relações públicas.

Por tudo isto, a segurança da informação contra potenciais incidentes ou ataques de segurança deve ser incluída nas prioridades estratégicas de qualquer organização e ser encarada como um processo contínuo e não algo pontual. Há que identificar possíveis riscos, nomeadamente vulnerabilidade técnicas, há que implementar e adotar controlos, há que realizar testes de intrusão persistentes e é aqui que a INTEGRITY pode fazer a diferença e tem vindo, nos últimos 12 anos, a acrescentar valor junto dos seus clientes. Como? Através da prestação de um serviço de excelência e inovador por parte de uma equipa de profissionais Expert e Seniores que, com a sua elevada experiência, contribuem para a segurança da informação.

Apenas salientar que cada gráfico apresentado terá uma legenda e respetiva análise dos indicadores, feita com base no know-how dos consultores da INTEGRITY, que dominam as especificidades dos setores analisados, tendo ainda tido o cuidado de explicar o significado de determinadas siglas e termos mais técnicos.



Pentesting

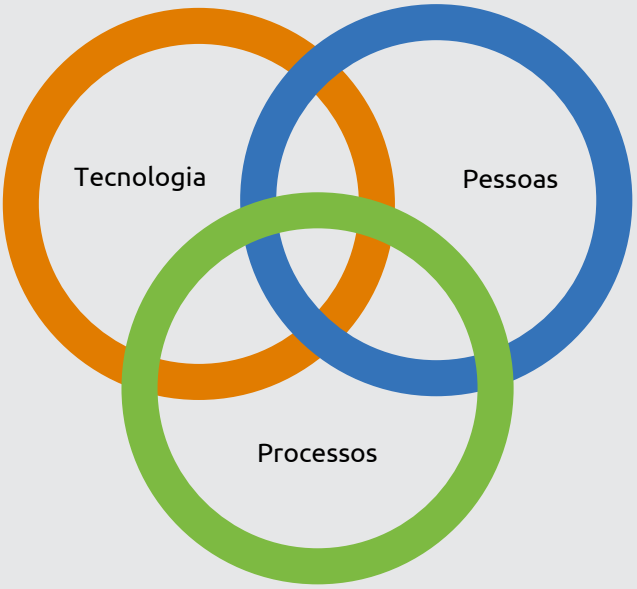
Numa sociedade cada vez mais virada para o digital, onde as tecnologias da informação têm um papel preponderante na vida das pessoas e nos negócios, torna-se absolutamente prioritária a questão da segurança da informação.

É sabido que a informação é o ativo estratégico mais importante das organizações, logo há que garantir, de forma eficaz, a sua segurança, evitando que terceiros consigam aceder, extrair, manipular e/ou destruir esse "bem" incomensurável.

Com o aumento do número de ciberataques a par da complexidade das advertências, as organizações têm vindo a aperceber-se da urgência em delinear uma estratégia no âmbito da **Gestão da Segurança da Informação**.

Uma das coisas que se pode desde logo fazer, anual ou semestralmente, são os Testes de Intrusão ou Pentests (Penetration Tests) que têm como objetivo testar as defesas dos sistemas e aplicações aos olhos de um potencial atacante. Realizados geralmente por entidades independentes e externas, nestes testes utilizam-se as metodologias e ferramentas que um típico *hacker* utiliza, porém de forma controlada. Quanto aos resultados, estes vêm todos descritos num relatório, com a explicação das vulnerabilidades identificadas e as recomendações para as corrigir.

Estamos perante três elementos que se articulam e relacionam entre si: **a tecnologia, as pessoas e os processos**, levantando-se questões tais como:
- De que forma está a funcionar a interação destes 3 elementos?
- Qual a eficiência destes controlos?



Uma coisa é certa: **é fundamental testar para perceber o ROI (Return on Investment)**.

Pentesting é a abordagem prática para testar de forma preventiva.

KEEP-IT-SECURE-24 Overview

A abordagem da INTEGRITY consiste em propor um serviço dinâmico e continuado, denominado de KEEP-IT-SECURE-24, que tem como objetivo a realização continuada e persistente de testes de Segurança da Informação na Infraestrutura, com grande enfoque na camada aplicacional de forma a detetar e corrigir atempadamente quaisquer eventuais vulnerabilidades de segurança que existam.

Nesta era digital, indivíduos e organizações estão todos mais expostos e, por isso, mais vulneráveis. Estão sempre ligados e acessíveis. A distância física deixou de ser um entrave, pois através de qualquer dispositivo consegue-se aceder, comunicar, resolver e fazer acontecer. E tudo isto de forma rápida, ágil e eficiente. A tecnologia veio de facto simplificar a vida das pessoas, proporcionando elevados níveis de dinâmica e organização. No entanto, todas estas vantagens acarretam vários riscos, que têm que ser adequadamente geridos.

É muito importante que dentro das organizações haja a noção de que devem procurar sempre manter a integridade da informação por si processada. Qualquer informação deve ser protegida no que concerne à Confidencialidade, Integridade e Disponibilidade, de forma a evitar danos à sua imagem, perda de receita, coimas ou outros impactos negativos.

Para uma organização ter noção daquilo que aconteceria caso os seus sistemas ou aplicações fossem atacadas e quais os dados que estariam em risco, pode recorrer ao **KEEP-IT-SECURE-24**, que disponibiliza uma equipa profissional de auditores certificados que fazem, de forma regular e persistente, testes aos seus sistemas e aplicações, disponibilizando uma Plataforma de Gestão Online para que a organização possa medir, gerir e corrigir as suas vulnerabilidades, possibilitando uma redução efetiva dos seus níveis de risco.

Atualmente as infraestruturas e aplicações são muito dinâmicas dada a sua necessidade constante de adaptação aos requisitos de negócio, o que faz com que haja necessidade de fazer alterações, as quais acabam por expor a organização a novas vulnerabilidades. O objetivo do serviço **KEEP-IT-SECURE-24** é testar o impacto das alterações na sua Segurança.

É de mencionar que se trata de um trabalho especializado e executado por consultores Seniores, para maximizar a qualidade dos resultados em particular ao nível da camada aplicacional e lógica de negócio.

KEEP IT SECURE 24

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

Tal como constatado, os testes efetuados no âmbito do KEEP-IT-SECURE-24 têm como alvo os sistemas e aplicações dos clientes, sendo feitos por uma equipa de profissionais qualificados e certificados para o efeito.

O objetivo das atividades de testes passa pela identificação de potenciais vulnerabilidades, utilizando ferramentas e metodologias similares aos potenciais atacantes, permitindo à organização efetuar a gestão e redução do risco de forma mais efetiva.

PenTesting Overview 2020

Enquadramento das Métricas

A elaboração deste relatório tem como base um data-set anónimo do qual foi obtida a informação determinante e relevante para análise.

Entidades

O portefólio de entidades clientes da INTEGRITY é alargado com referências tanto no mercado nacional como internacional, tendo como clientes alvo as grandes e médias empresas dos mais variados setores, no entanto o presente relatório focar-se-á sobre os setores Financeiro, Indústria & Energia e Serviços.

O setor Financeiro é um setor tipicamente mais maduro na aplicação de práticas de cibersegurança, derivado das obrigações e regulamentações a que está sujeito e da especificidade da atividade destas entidades.

As entidades enquadradas no setor de Indústria & Energia são grandes organizações sensíveis aos riscos e ameaças a que a sua atividade está sujeita.

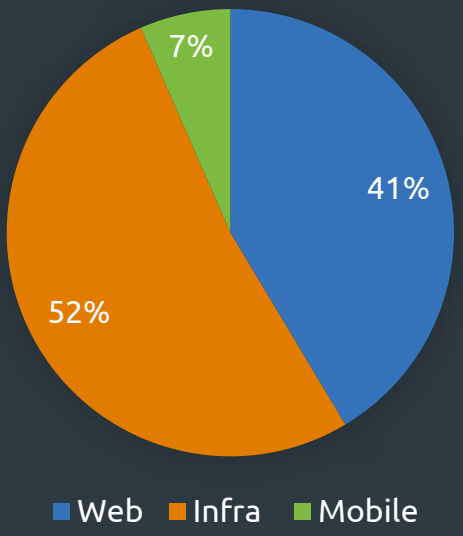
No setor dos Serviços a amplitude de entidades é maior, havendo níveis diversos de exposição ao risco, mas que são encarados como prioritários para a proteção da continuidade do negócio.

Sobre os Assets

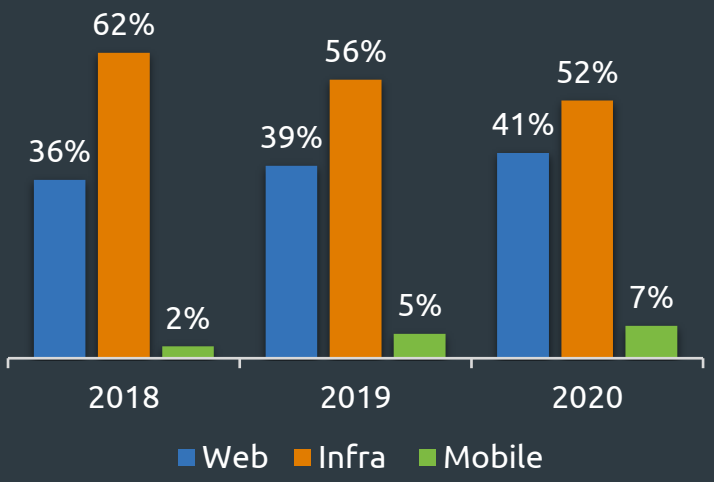
Os assets (ativos) são sistemas, redes ou aplicações visadas pelo Serviço de Pentesting.

O Pentesting executado em 2020, no âmbito do KEEP-IT-SECURE-24, incidiu sobretudo nos 3 tipos de assets abaixo apresentados: Infraestrutura, com a percentagem mais elevada (52%), Web (41%) e Mobile (7%).

Distribuição dos Tipos de Assets



Tipologia de Assets Testados



Tendências de Mobile APPS

Ao analisar o gráfico, este indica que nos últimos 3 anos há uma tendência crescente na evolução de assets a teste nas vertentes de Web e Mobile, apresentando as Infraestruturas uma tendência decrescente.

Este aumento nas vertentes Web e Mobile acompanha uma tendência geral de aumento de exposição de serviços online. No que diz respeito aos clientes da INTEGRITY verifica-se que estes disponibilizam cada vez mais serviços nos seus canais online, nomeadamente websites e mobile. É indiscutível que, nos últimos anos, houve um reforço da presença das organizações no panorama digital, o que justifica o interesse em testar, sobretudo estas duas áreas.

Quanto às Infraestruturas, o seu decréscimo reflete a passagem de parte da infraestrutura dos clientes da INTEGRITY para serviços da cloud em modelo de SaaS ou IaaS.

Ou seja, a partir do momento em que a infraestrutura pertence a um fornecedor de cloud e é partilhada, ela deixa de ser o alvo primordial de testes e o foco passa a ser a componente aplicacional restrita ao cliente em causa, daí o número de assets de Infraestrutura estar a baixar, tal como se verifica no gráfico.

Por outro lado, o crescimento na utilização de micro-serviços e "containerization" leva a que apesar de existir maior complexidade técnica, a exposição de serviços seja restrita ao que realmente é necessário, ao funcionamento da aplicação. Em algumas circunstâncias a tendência de passagem para micro-serviços vê-se acompanhada com a passagem para a cloud, fatores que levam ao decréscimo de assets de infraestrutura a teste no serviço KEEP-IT-SECURE-24.

Vulnerabilidades

A realização de testes de intrusão é uma prática avançada quando se fala em Segurança da Informação. Existem diversas vulnerabilidades a que organizações e utilizadores em trabalho remoto estão expostos, e o mercado tende a destacar determinados tipos de ataque em momentos específicos. Conforme o nível de severidade de vulnerabilidades existem práticas de resolução específicas que, quanto mais atempada for a sua deteção, maior será a garantia de segurança da informação.

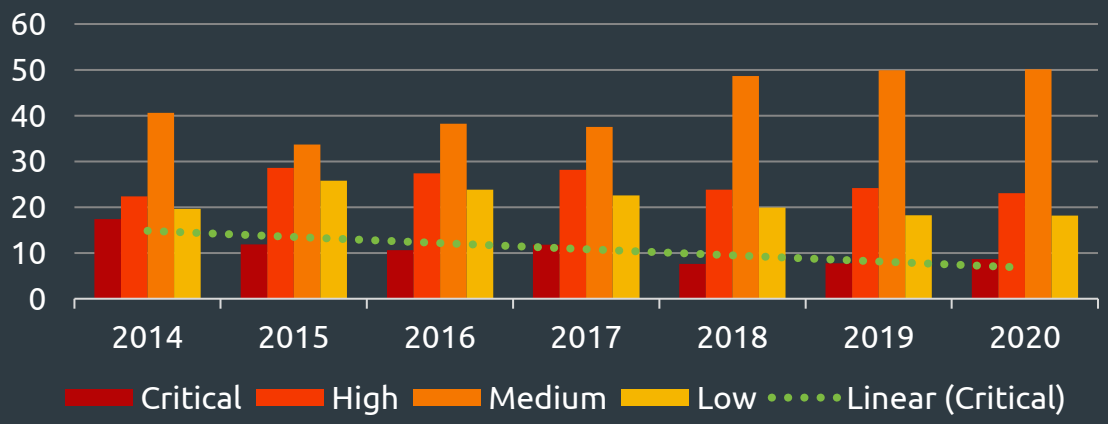
Severidade das Vulnerabilidades

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.

As severidades do nível **HIGH ou CRITICAL** indicam que o impacto potencial nos sistemas ou informação é elevado.

Evolução da Severidade por Vulnerabilidades de 2014 a 2020



Tal como se pode ver no gráfico, ao longo dos últimos sete anos há uma ligeira tendência de decréscimo nas vulnerabilidades Critical, o que demonstra uma maturidade crescente de algumas organizações ao longo tempo, que faz com que tendencialmente tenham cada vez menos vulnerabilidades Critical. De notar que o turnover de clientes é extremamente reduzido, o que faz com que determinadas organizações contribuam de forma positiva para o valor global.

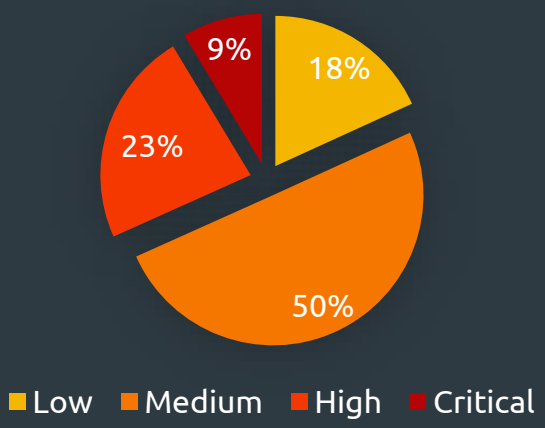
O decréscimo de vulnerabilidades críticas está também relacionado com a utilização generalizada de Frameworks, que incorporam controlos de segurança e mitigam de forma "automática" uma parte das vulnerabilidades mais comuns relacionadas. A implementação de metodologias de desenvolvimento, que contemplam a segurança durante o decorrer do ciclo de vida de desenvolvimento, contribuem também para o decréscimo de vulnerabilidades de maior severidade.

Na verdade, a partir do momento em que a organização começa a trabalhar com a INTEGRITY, vai tendo cada vez mais sensibilidade e os seus processos vão efetivamente melhorando, logo há a tendência de redução da introdução de vulnerabilidades Critical.

As vulnerabilidades de severidade Medium e Low, apesar de serem as que merecem menos atenção, continuam a ser relevantes e são a fatia onde mais facilmente caem vulnerabilidades.

A percentagem de vulnerabilidades Medium tem-se mantido estável, no entanto em 2018 verificou-se uma subida relativa relacionada com o decréscimo de vulnerabilidades Critical e consequentemente o aumento percentual das restantes e também ao aumento substancial de vulnerabilidades relativas à implementação de TLS (Transport Layer Security) nomeadamente pela utilização de cifras consideradas fracas e, como tal, desaconselhadas.

Distribuição das Vulnerabilidades por Severidade no Decorrer de 2020



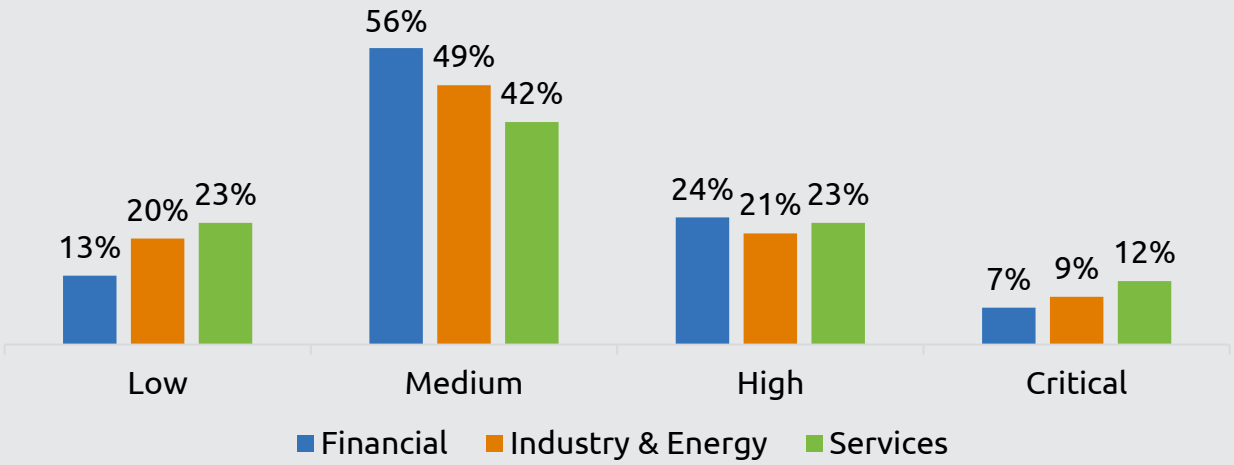
O gráfico acima demonstra que há claramente uma percentagem maior nas vulnerabilidades com severidade Medium (50%), exatamente por refletirem temas de impacto mais reduzido e de exploração mais difícil ou pouco útil da perspetiva de um atacante.

Quanto aos 9% registados nas vulnerabilidades com severidade Critical, apesar de poder parecer um valor reduzido percentualmente, é de referir que, em termos práticos, cada uma das vulnerabilidades identificadas com esta severidade coloca em causa, de forma objetiva e direta, sistemas ou aplicações, e consequentemente a informação de uma organização.

Nas vulnerabilidades Critical o impacto e a facilidade de exploração são tipicamente bastante elevados. É, na verdade, muito frequente que um atacante que explore uma destas vulnerabilidades não fique circunscrito ao sistema "onde estas vivem", permitindo uma progressão para outros sistemas ou aplicações, e mantendo posteriormente persistência dentro da organização. Por vezes, a exploração de uma vulnerabilidade de severidade Critical permite a um atacante externo chegar à rede interna e desencadear ações com intuito malicioso, como por exemplo campanhas de ransomware. Por tudo isto há que considerar relevante o valor de 9%.

Nível de Severidade por Setor:

Financeiro, Indústria & Energia e Serviços



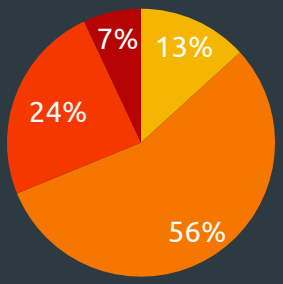
Tal como se pode constatar, o setor Financeiro é aquele que tem menor número de vulnerabilidades com severidade Critical, o que reflete um nível de maturidade superior relativamente aos outros setores.

O setor Financeiro é um setor que tradicionalmente se preocupa com a segurança, por ser normalmente um dos mais visados pelas fraudes, ataques de malware e phishing, tendo por isso já alguns processos instituídos e apostado na adoção de medidas de prevenção de riscos, o que acaba por torná-lo menos vulnerável.

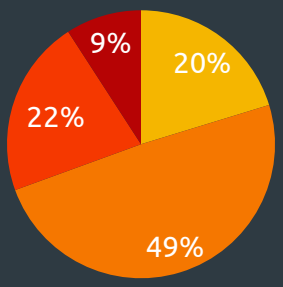
O setor da Indústria & Energia apresenta uma severidade Critical abaixo do setor dos Serviços, o que poderá estar relacionado com o facto de ser um mercado com menor exposição online no que diz respeito à interação com os seus clientes finais.

Quanto ao setor dos Serviços é aquele que apresenta maior número de vulnerabilidades com severidade Critical, por abarcar mais tipo de negócios e por ter um conjunto de clientes mais heterogéneo e com maior exposição online no que diz respeito a serviços prestados aos respetivos clientes.

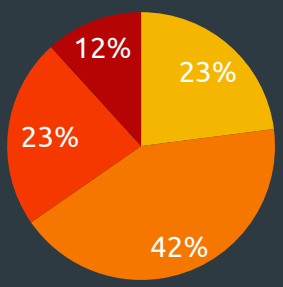
Nível de Severidade no Setor Financeiro



Nível de Severidade no Setor Indústria & Energia

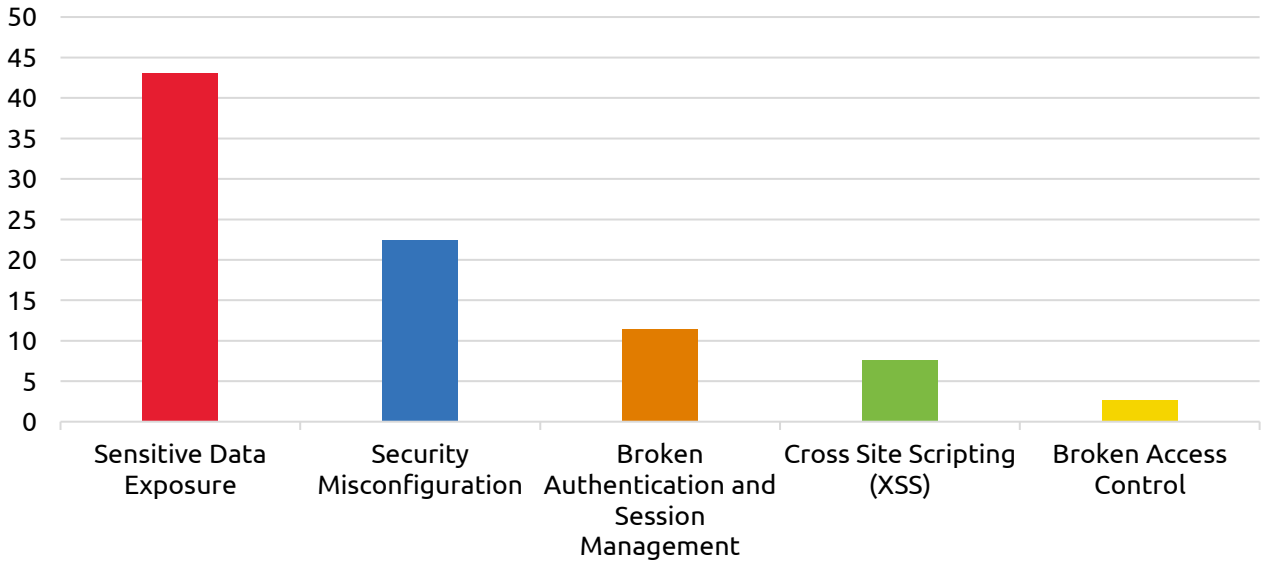


Nível de Severidade no Setor dos Serviços



Top Tipos de Vulnerabilidades

Tipos de Vulnerabilidades mais comuns - 2020



Através deste gráfico, constata-se que o **Sensitive Data Exposure** é a vulnerabilidade mais comum em todo o espectro de clientes da INTEGRITY.

Sensitive Data Exposure

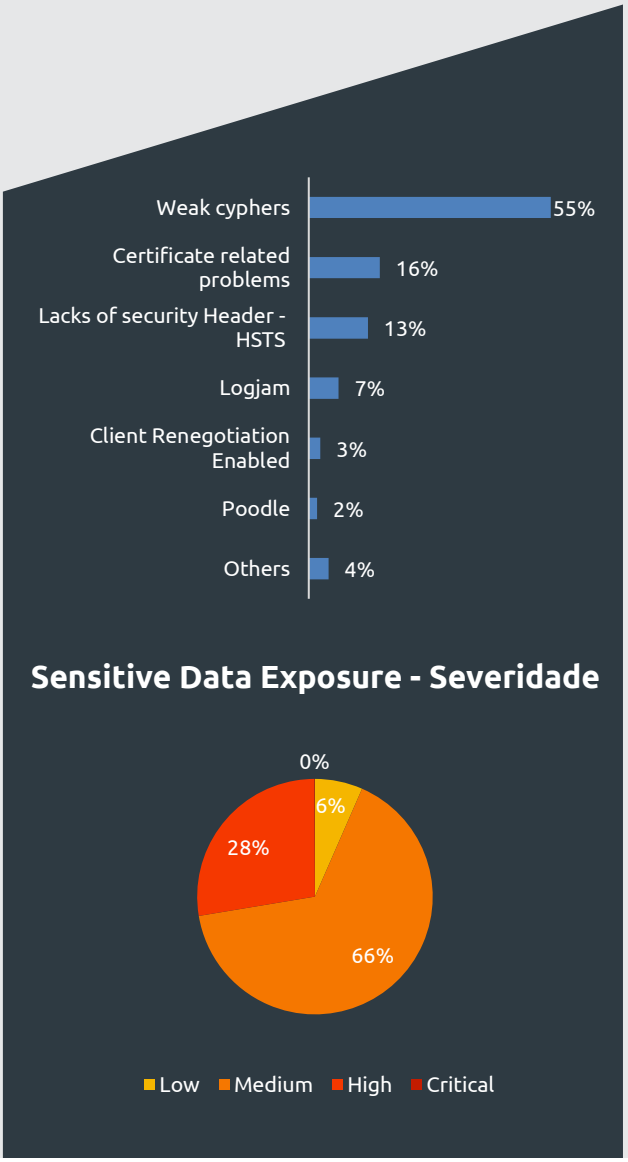
A Informação Sensível é informação que, pela sua natureza, deve estar protegida de acesso não autorizado. **Sensitive Data Exposure** acontece quando a informação sensível não é adequadamente protegida em trânsito. Na sua maioria, este tipo de vulnerabilidades é observada na sequência de ausência ou erros na configuração do protocolo Transport Layer Security (TLS), que fornece uma camada de transporte que, quando bem implementada, garante a integridade e confidencialidade de dados.

Na sua maioria tratam-se de vulnerabilidades de severidade Medium e High, atendendo a que a exploração de muitas delas não é fácil e, consequentemente, pouco provável de ocorrer na realidade.

Este é um problema que se repete ano após ano, pois apesar da aparente simplicidade da configuração do protocolo, na prática revela-se como uma tarefa muito complicada, existindo muita informação dispersa, pouco fidedigna ou desatualizada relativamente à implementação das melhores práticas, o que acaba por não ajudar.
Por outro lado, observa-se que é por vezes complicado implementar as best practices, sem colocar em causa a continuidade do serviço para determinadas franjas de clientes que utilizam tecnologias mais antigas.

Em 55% das vulnerabilidades de Sensitive Data Exposure vê-se a utilização de Cifras Fracas, ou seja, cifras que foram consideradas vulneráveis ou pouco seguras.

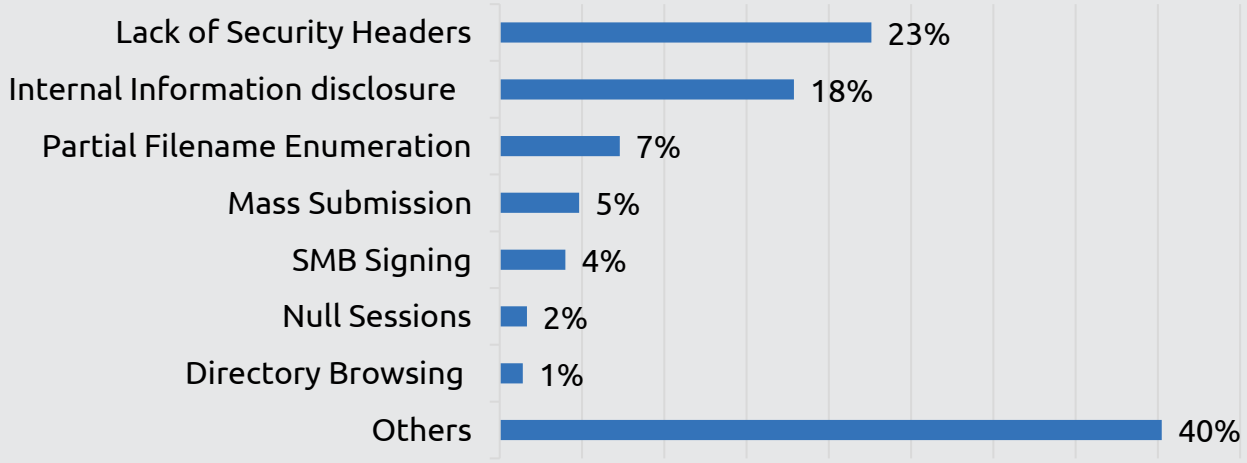
A ausência do header de Strict-Transport-Security (HSTS), que confere à comunicação um nível acrescido de resiliência a ataques de MITM (man-in-the-middle), verifica-se em 13% das vulnerabilidades de Sensitive Data Exposure.



Recomendações

- *Classificação da informação armazenada e transmitida por cada aplicação para garantir que os dados sensíveis são identificados, são cumpridos todos os requisitos legais e de negócio e são aplicados os controlos adequados.*
- *Utilizar algoritmos fortes e standard para o transporte e armazenamento da informação.*
- *Definir diretivas internas relativamente a protocolos e cypher-suites suportados, tendo em consideração os requisitos de negócio, a sensibilidade da informação e suporte desejado aos utilizadores finais das aplicações.*

Security Misconfiguration



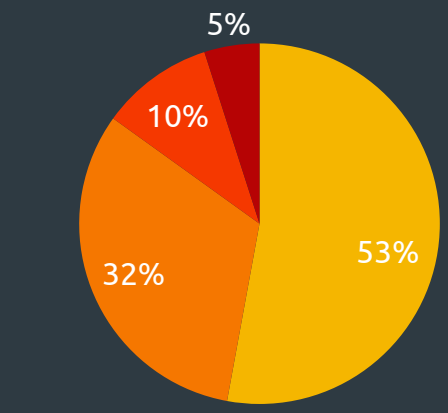
O **Security Misconfiguration** é o segundo tipo de vulnerabilidade mais comum e que, engloba configurações incorretas que afetam a segurança dos sistemas ou aplicações. Este tipo de vulnerabilidade regista uma tendência crescente que acompanha o aumento de complexidade e heterogeneidade nos sistemas, redes e aplicações, que consequentemente se reflete também no aumento de controlos disponibilizados nas Frameworks que suportam as aplicações, nos sistemas operativos e redes, tornando-se necessário mais conhecimento técnico para efetuar as configurações adequadas.

Consequentemente, a probabilidade do erro humano aumenta na implementação dos controlos. As configurações de segurança presentes de base nos componentes que compõem as soluções são eficazes para alguns dos problemas mais comuns, mas existe muitas vezes a necessidade de otimização para o caso particular.

O tipo de vulnerabilidade Security Misconfiguration engloba várias vertentes como redes, webservers, application servers e sistemas.
No que diz respeito a esta vulnerabilidade em 2020, pode-se observar que 25% das incidências consistem na disponibilização inadvertida de informação interna ao utilizador/atacante. Por exemplo, em respostas ou *stack traces* contendo endereços IP ou *paths* internas. Ainda é possível observar em 7% das situações a existência de uma vulnerabilidade de 2010 no software IIS (Internet Information Services) que permite a enumeração de ficheiros ou diretórios utilizando o símbolo "~", utilizado para garantir retro compatibilidade.

Outros 23% das vulnerabilidades são relacionadas com a ausência ou erro de configuração de headers de segurança, como por exemplo X-Frame-Options que evita que uma página seja apresentada numa iframe ou ausência de Cache-control que permite dar indicação ao browser para não fazer cache de informação sensível contida na resposta.

Security Misconfiguration - Severidade



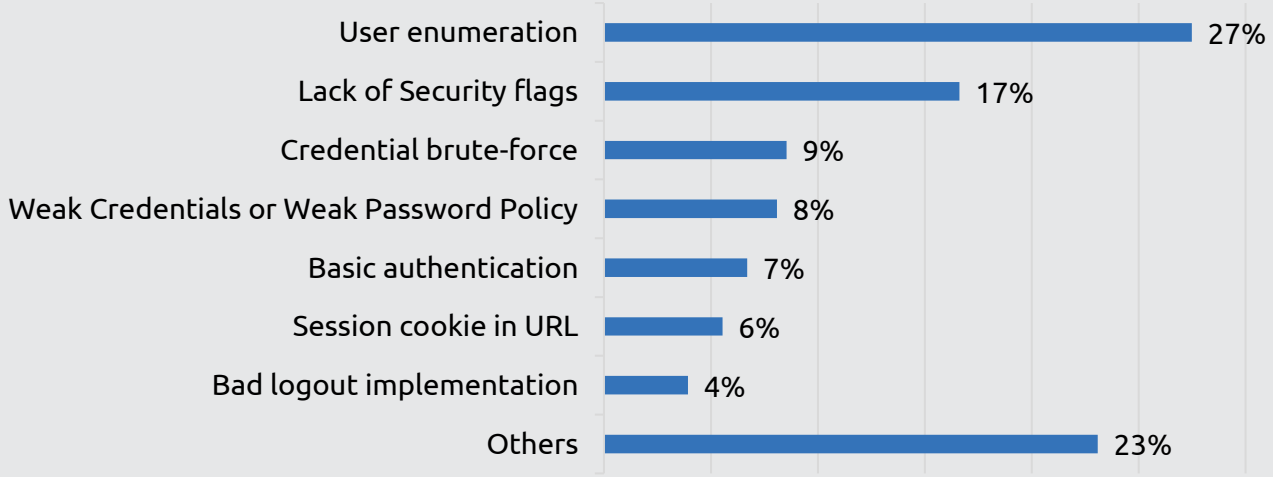
Outra das vulnerabilidades comuns (5%) é a utilização de protocolos e aplicações que permitem a submissão em massa de informação para as aplicações ou sistemas.

No contexto das redes internas, as falhas mais comuns no que diz respeito ao **Security Misconfiguration** são as Null Sessions e o Smb Signing desativo.

As vulnerabilidades de Security Misconfiguration encontram-se dispersas por todas as severidades, no entanto cerca de 85% delas são de severidade Medium e Low.

Apesar de na generalidade este tipo de vulnerabilidade não apresentar severidade Critical, existem algumas situações que se revelaram dramáticas, como por exemplo a existência de credenciais por omissão de administração, disponibilização de interfaces de debugging, existência de credenciais nos stack-traces ou, no caso de redes internas, quando a ausência de SMB Signing em conjugação com uma política de passwords fraca permite a obtenção de privilégios.

Broken Authentication and Session Management

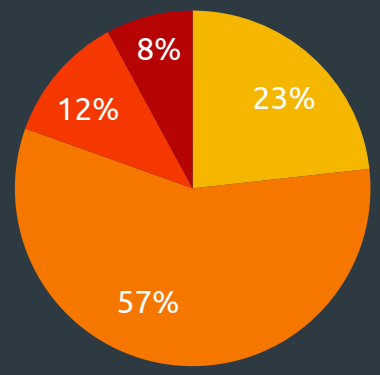


O **Broken Authentication and Session Management** é focado na componente de autenticação e gestão de sessão dos utilizadores de uma aplicação que, quando exploradas com sucesso, permitem a um atacante o acesso ilegítimo às aplicações e sistemas. Este tipo de problema surge, por vezes, devido a falhas de desenho dos sistemas em causa, mas também na falha de configuração de controlos de segurança já incluídos de base nos sistemas.

No decorrer do ano de 2020 foi observado que cerca de 27% das vulnerabilidades registadas com este tipo se referem à enumeração de utilizadores, ou seja, a possibilidade de um atacante, na sua maioria das vezes de forma não autenticada, ter a possibilidade de aferir a existência de determinado utilizador num sistema ou aplicação. Só por si, esta vulnerabilidade não apresenta risco imediato, no entanto permite a um atacante desencadear por exemplo ataques de brute-force ou password spraying. De facto, 9% das vulnerabilidades referentes a Broken Authentication and Session Management referem-se à possibilidade de executar brute-force, sem que qualquer mecanismo de deteção ou prevenção seja desencadeado pela aplicação.

Tal como se constata, nos tipos mais comuns listados anteriormente, registam-se também aqui a ausência de algumas configurações como por exemplo a flag Secure ou a HTTP-Only que tem como objetivo evitar que o código JavaScript que corre no browser do utilizador possa aceder a determinada cookie, minimizando a possibilidade de roubo (hijack) de sessão, através por exemplo de um ataque de Cross-Site-Scripting.

Broken Authentication and Session Management - Severidade



No Broken Authentication and Session Management as severidades distribuem-se por todos os níveis, mas com maior prevalência para Medium.

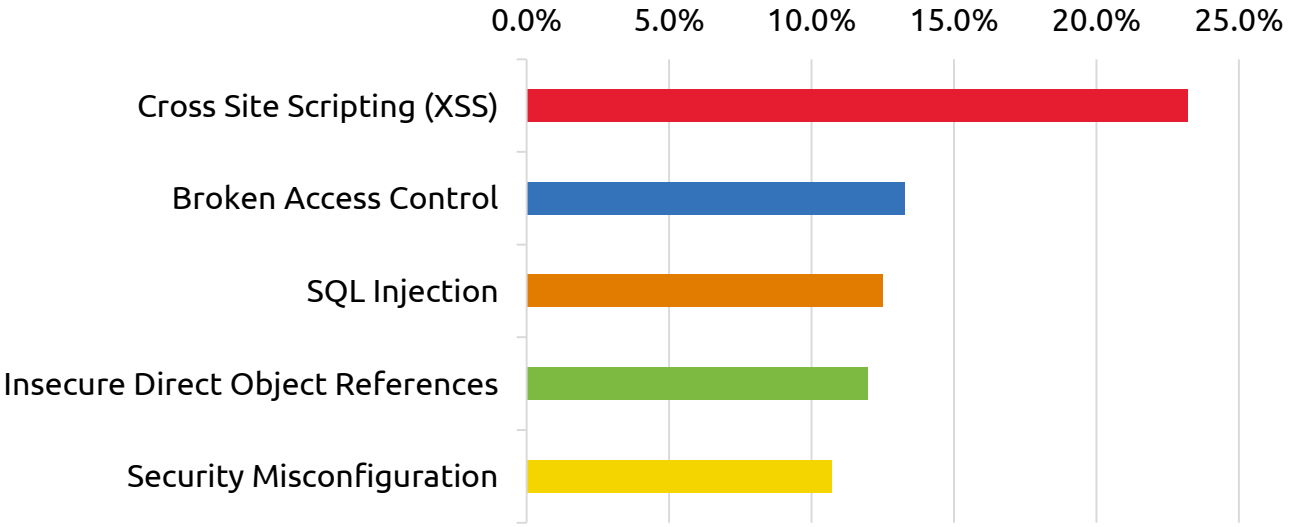
Existem porém algumas circunstâncias em que vulnerabilidades deste tipo colocam em causa, de forma severa, a segurança dos sistemas e informação. Em 2020,8% das vulnerabilidades relativas a este tipo de forma de severidade Critical. Destacam-se algumas delas em que foi possível aceder com passwords aleatórias, sem credenciais em consolas de administração, utilizando passwords previsíveis, ou usando JSON Web Tokens não assinados ou com chaves conhecidas.

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.*
- *Manter boas políticas de passwords.*
- *Geração de um session ID Aleatório após o login.*
- *Implementação adequada de expiração de sessões (timeout).*

Vulnerabilidades Críticas mais Comuns

As vulnerabilidades com severidade Critical, apesar de ocorrerem em menor número de vezes, são aquelas que, devido ao seu impacto, mais facilmente colocam em causa a segurança dos sistemas e aplicações. Por este motivo é importante fazer uma observação focada apenas neste grupo.



O gráfico enumera os **Tipos de Vulnerabilidades Críticas mais Comuns**, sendo que abaixo será feita uma análise pormenorizada sobre as três primeiras vulnerabilidades críticas mais comuns.

Top 3 de Vulnerabilidades Críticas

Cross Site Scripting

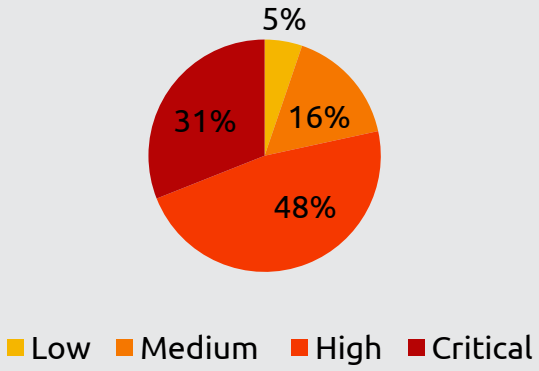
Consiste numa vulnerabilidade em que código JavaScript malicioso é injetado no contexto de um acesso a um site benigno. A injeção pode ser efetuada diretamente no URL, através da adição de código malicioso que quando for processado pelo site será enviado para o browser e acedido pela vítima (Reflected Cross-Site-Scripting) ou, noutros casos, pode ser colocado no servidor de forma permanente (Stored Cross-Site-Scripting) e é consumido pela vítima numa simples navegação do website. Ao executar código JavaScript no contexto da vítima, o atacante poderá obter informação sobre a sua sessão e no extremo, efetuar o login no contexto da sessão da vítima. O código gerado pelo atacante pode realizar uma grande diversidade de ações, como roubar a sessão, ou mesmo efetuar keylogging.

Esta vulnerabilidade pode ser desencadeada induzindo a vítima a submeter o pedido gerado pelo atacante de variadas formas. O atacante pode, por exemplo, enviar à vítima um link contendo um URL malicioso, no contexto de um email ou de uma mensagem instantânea. Pode ainda submeter este link para websites populares que permitam a publicação de conteúdos, por exemplo, através de um comentário num blog. Também poderá criar um website aparentemente inócuo, mas com a capacidade para levar qualquer utilizador que o visite a executar pedidos entre aplicações/sites diferentes (cross-domain) dirigidos à aplicação vulnerável.

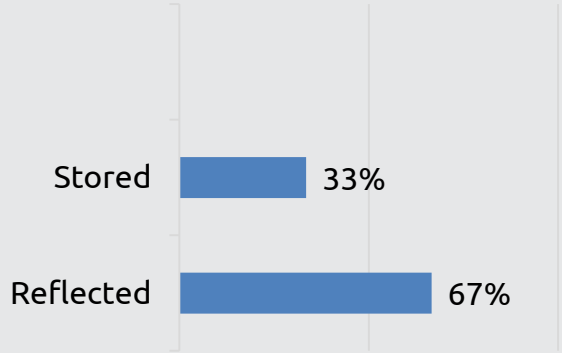
O Cross Site Scripting Reflected e Stored podem ser endereçados através da filtragem de input, encoding de output e estabelecimento de regras restritivas relativamente à colocação de informação não confiável proveniente do utilizador, de forma a evitar que JavaScript seja introduzido e executado no contexto da página web carregada pela vítima de forma não esperada.

As severidades deste tipo de vulnerabilidade distribuem-se por diversos níveis, atendendo por exemplo à necessidade de interação da vítima para o sucesso do ataque como é o caso do Reflected XSS, ou na abrangência do ataque e na sua capacidade de afetar múltiplas vítimas de uma vez só como é o caso por vezes no Stored XSS. A informação em causa no ataque e o facto de ser desencadeado em contexto autenticado é também relevante para a sua severidade.

Cross Site Scripting - Severidades

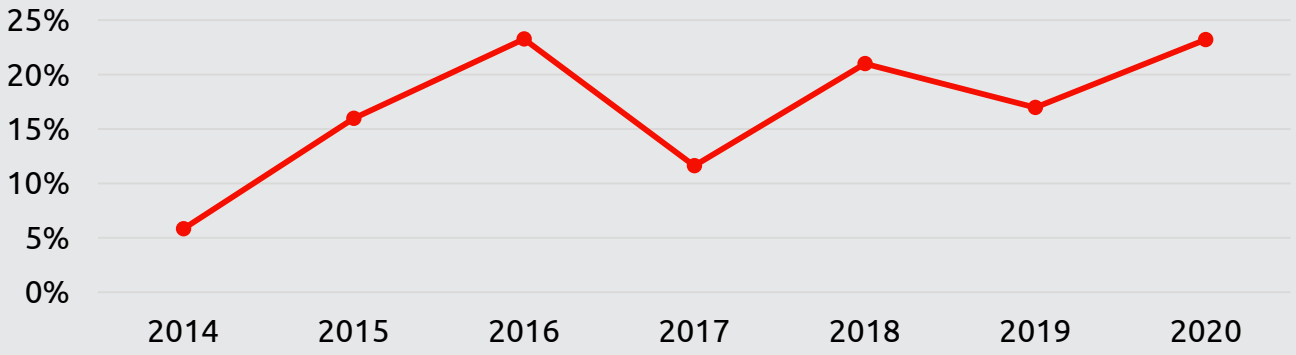


Cross Site Scripting - Types



Em relação a esta vulnerabilidade, há que referir que se tem vindo a assistir a um aumento de incidências que pode estar relacionado com o aumento de complexidade das soluções de software. Com a passagem para soluções de micro-serviços ou outras soluções muito modulares, a resolução deste tipo de problema pode tornar-se algo complexa, atendendo a que cada módulo poderá não ter o contexto aplicacional suficiente sobre o fluxo, nomeadamente o local onde será apresentada a informação que está a processar para efetuar de forma assertiva a codificação adequada.

Cross Site Scripting - Evolução



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 conter apenas letras (acentos incluídos) e espaços, emails devem respeitar a norma RFC 5322 (3.4.1. Addr-spec specification - pág. 17), entre vários outros tipos de dados.*
- *Devem ser aplicados filtros de encoding e escaping do output para HTML, tais como OWASP ESAPI, ou Microsoft AntiXSS Library.*
- *O cabeçalho HTTP Content-Security-Policy deve ser definido de maneira a, por exemplo, executar apenas scripts disponíveis no domínio atual (script-src 'self') e negar scripts inline, bem como implementar subresource integrity.*

Broken Access Control

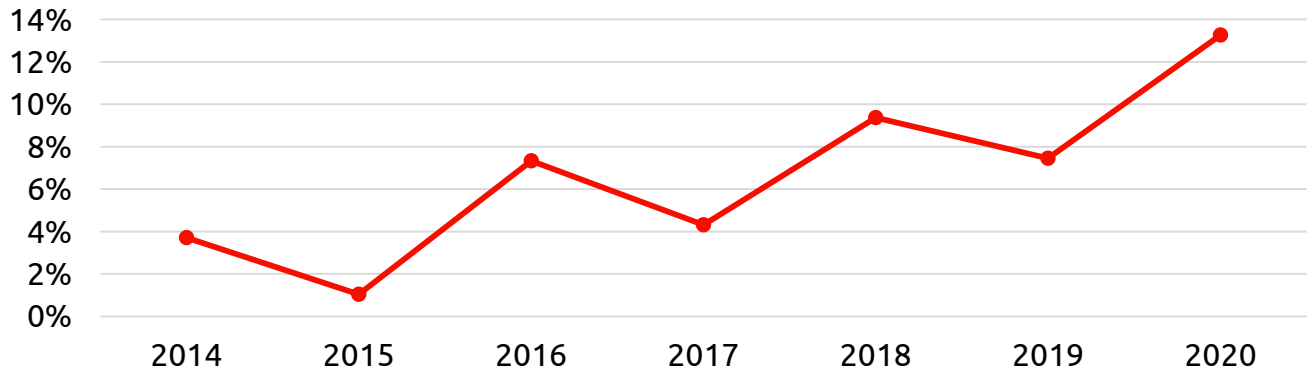
O controlo de acessos é o mecanismo implementado, após a autenticação, para garantir que a autorização de acesso aos conteúdos e funções presentes numa aplicação ou sistema é permitido apenas aos utilizadores adequados.

A implementação é complexa e deve ser alvo de forte ponderação e estabelecimento prévio de uma política de controlo de acessos. Quando este controlo é suportado em código espalhado por vários locais da aplicação, código pouco modular e por regras ad-hoc, poderão estar lançadas as sementes para a existência de vulnerabilidades deste tipo.

O impacto de uma vulnerabilidade de Broken Access Control pode ser devastadora quando por exemplo um utilizador tem acesso a informação sensível de outro ou obtém privilégios de administração sobre um sistema.

O teste ao controlo de acessos não é uma tarefa fácil. Para o sucesso dos testes há que conhecer a lógica da aplicação bem como as regras negócio e de acesso que ditam que um utilizador deve ter acesso a algo e o outro não."

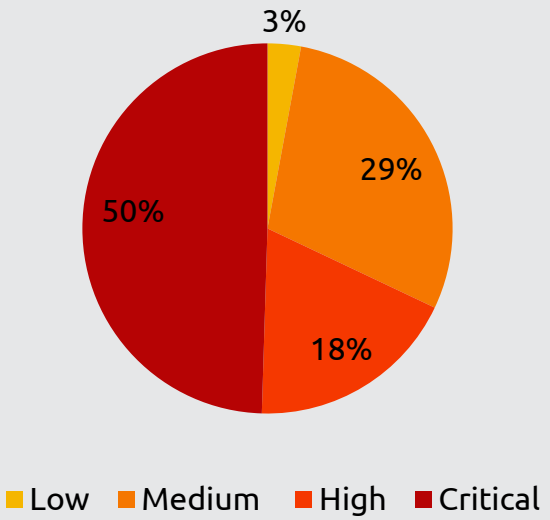
Broken Access Control - Evolução



O gráfico demonstra uma tendência crescente do **Broken Access Control** que poderá ser motivada pelo aumento de complexidade e de número de aplicações que disponibilizam funcionalidades autenticadas aos seus utilizadores. Por outro lado, o controlo de acesso não é algo que possa ser consumido diretamente das frameworks sem que haja desenvolvimento específico para as necessidades apresentadas caso a caso.

Broken Access Control - Severidades

No que diz respeito às severidades, o gráfico abaixo demonstra que 50% das incidências são de severidade Critical. Pode-se concluir que quando se regista uma falha deste tipo o impacto é tipicamente bastante severo.



Em 2020 observaram-se diversas vulnerabilidades de Broken Access Control que consistiam no acesso a dados e funcionalidades destinadas a outros utilizadores e de forma indevida. Podendo-se, no entanto, destacar algumas das mais surpreendentes, como a possibilidade de atuar sobre máquinas virtuais ou criar outros utilizadores com acessos mais privilegiados ou até mudar as próprias permissões.

Recomendações

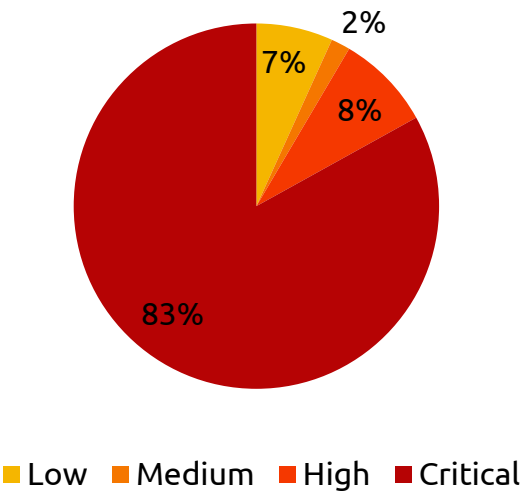
- *Desenhar a aplicação com base num modelo de acesso bem definido e de raiz, por exemplo role-based access control, de forma a minimizar inconsistências.*
- *Utilizar uma política de negar por omissão a não ser que a informação em causa seja pública.*
- *Forçar a que todos os pedidos passem pelo código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

SQL Injection

A vulnerabilidade de SQL injection consiste na inserção de código SQL em pontos controlados pelo atacante/utilizador, de forma a alterar o funcionamento desenhado do query que suporta a funcionalidade afetada. O impacto deste tipo de vulnerabilidades pode ir da leitura de conteúdos das bases de dados de forma indiscriminada, à destruição de dados ou mesmo ao controlo do servidor onde se encontra a base de dados.

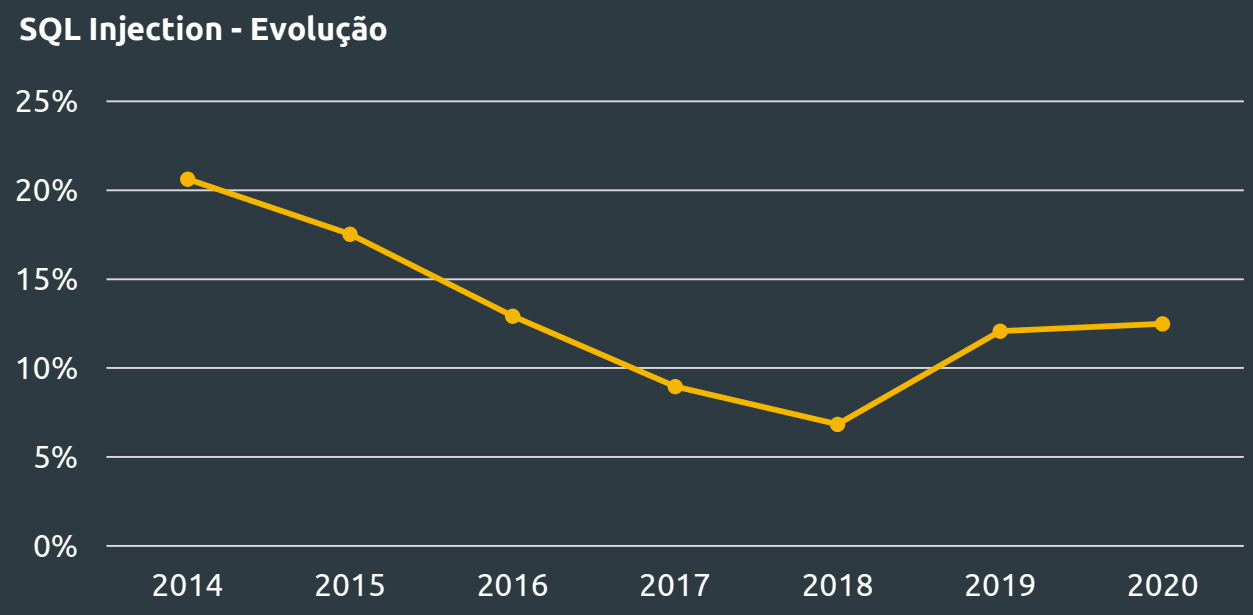
Das vulnerabilidades vistas até ao momento, o SQL injection é a que maior probabilidade de impacto crítico apresenta.

SQL Injection - Severidades



No que diz respeito às severidades, pode-se observar no gráfico acima que em 2020, quando explorado com sucesso, o SQL Injection refletiu-se num impacto muito severo em 83% das vezes.

O **SQL Injection** é um dos "pesos pesados" das vulnerabilidades mais crítica e, tal como se vê no gráfico, tem vindo a ter um decréscimo, justificado fundamentalmente pela utilização de frameworks que já implementam em si um conjunto de controlos que inibem o programador de produzir código errado (que potencia o SQL Injection). Esta diminuição poderá também estar relacionada com uma maior consciencialização dos programadores.



Recomendações

- *Utilização de 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.

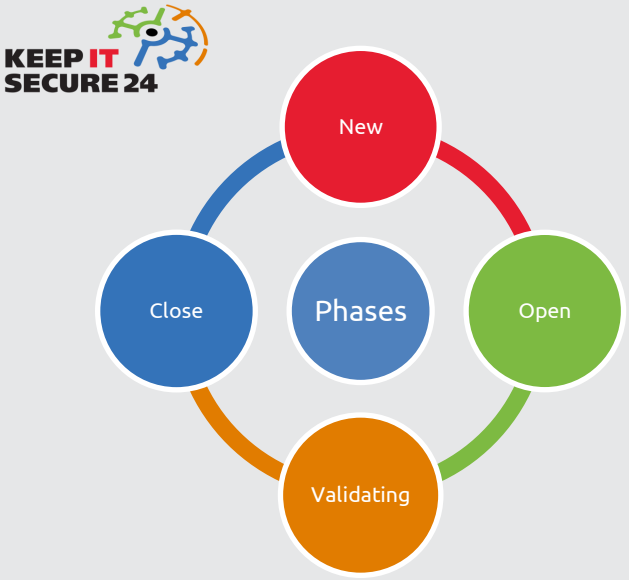
- *Filtragem e validação de dados:*
  Os dados oriundos de utilizadores, e sob seu controlo, devem ser validados pela aplicação quanto ao seu conteúdo.

- *Revisão de 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.

- *Formação aos 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 a resiliência das mesmas às falhas.

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.



O processo de resolução de vulnerabilidades passa por várias fases, desde a sua identificação e publicação na plataforma KEEP-IT-SECURE-24 (estado New), a abertura da vulnerabilidade por parte do cliente (estado Open), passando para a validação (estado Validating), terminando quando esta está resolvida (estado Close). Todavia, há que mencionar que, antes de entrar no estado Close, pode haver a chamada **reabertura** ou não, havendo aqui dois caminhos possíveis:

- A INTEGRITY chega à conclusão que a implementação dos controlos foi bem feita (e passa para o estado Close);
- A INTEGRITY chega à conclusão que o cliente não implementou bem os controlos, ou seja, continua a existir risco (e passa do estado Validating para o estado Open).

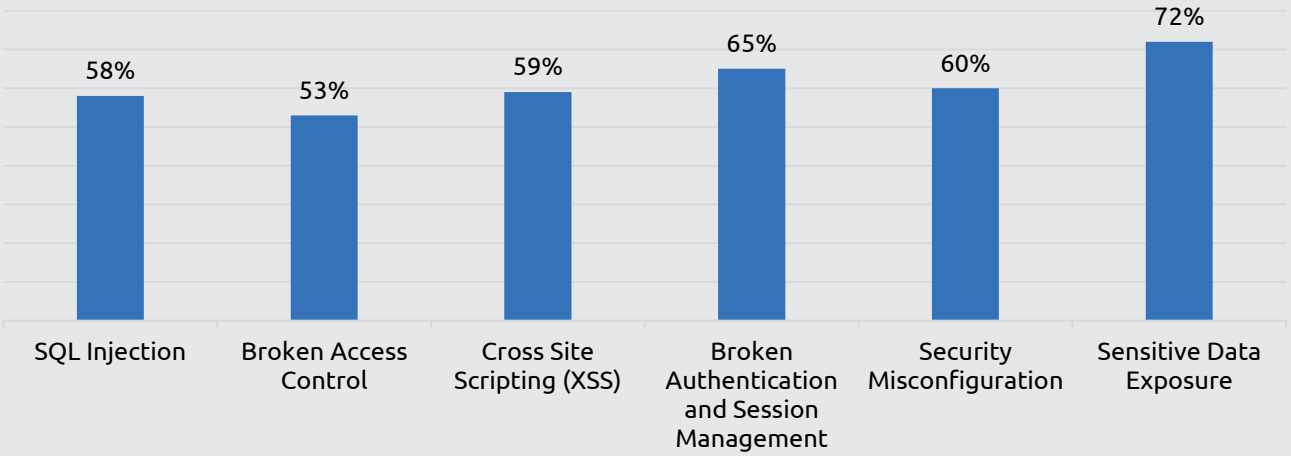
Para se compreender como melhorar os processos de resolução de vulnerabilidades há que avaliar as dificuldades de fecho associadas a determinadas vulnerabilidades. Uma das métricas a avaliar é o número de vezes que determinada vulnerabilidade foi dada como resolvida pelo cliente e que, após verificação da INTEGRITY foi reaberta por não se encontrar completamente resolvida.

No modelo KEEP-IT-SECURE-24 as vulnerabilidades são colocadas no estado de Validating, para dar indicação à INTEGRITY para retestar determinada vulnerabilidade que foi considerada resolvida.

Dificuldades de Resolução Efetiva

Vulnerabilidades que Registaram Reaberturas

Percentagem de vulnerabilidades que não foram resolvidas à primeira tentativa em 2020 para os tipos mais comuns.



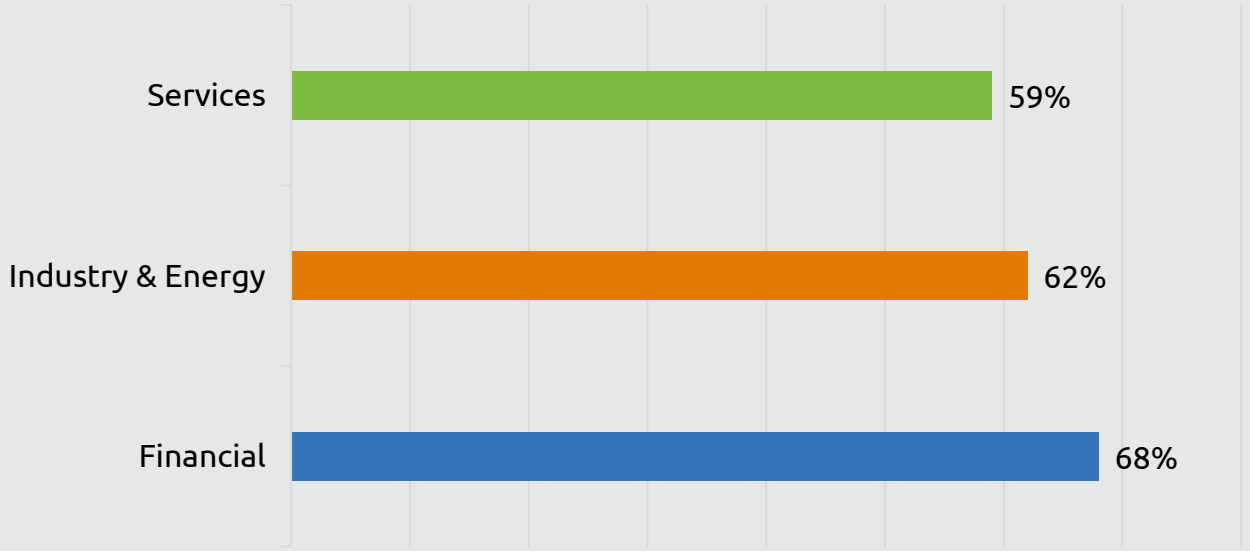
Verifica-se que, de forma transversal, todos os tipos de vulnerabilidades necessitaram de múltiplas iterações para a sua resolução efetiva.

Das vulnerabilidades mais comuns, listadas acima, a que maior dificuldade de fecho apresenta – traduzida na percentagem de vulnerabilidades com tentativas de resolução falhadas – é o Sensitive Data Exposure. Sendo um tipo composto de vários subtipos, é interessante fazer o zoom-in e verificar que 47% das vulnerabilidades deste tipo que não foram fechadas à primeira tentativa se referem a cifras fracas e que 19% se referem à implementação de HSTS (HTTP Strict Transport Security).

No que diz respeito ao grupo de vulnerabilidades enquadradas no Security Misconfiguration, as que maior dificuldade de fecho apresentaram foram IIS Partial Filename Enumeration e Implementação do header de X-Frame-Options.

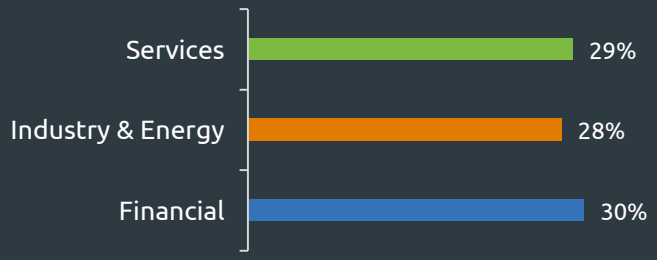
Relativamente ao tipo Broken Authentication and Session Management, a vulnerabilidade que se destacou das outras foi a enumeração de utilizadores.

Percentagem de Vulnerabilidades Reabertas por Setor



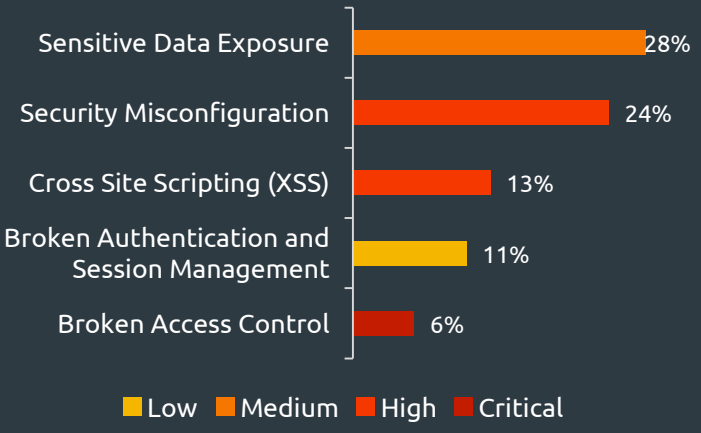
Este gráfico demonstra que todos os setores se encontram nivelados quanto à capacidade de fecho de vulnerabilidades à 1ª tentativa. O setor Financeiro apresenta resultados que revelam menor eficácia no fecho e o setor dos Serviços demonstrou em 2020 ser o setor mais assertivo no fecho das vulnerabilidades. A dimensão elevada das organizações e a quantidade de equipas envolvidas parece contribuir para uma menor eficácia.

Percentagem de Vulnerabilidades Resolvidas por Setor



No caso da percentagem de vulnerabilidades resolvidas face a vulnerabilidades identificadas em 2020, observa-se que ao contrário do gráfico anterior, o setor Financeiro encontra-se melhor posicionado na percentagem de vulnerabilidades resolvidas.

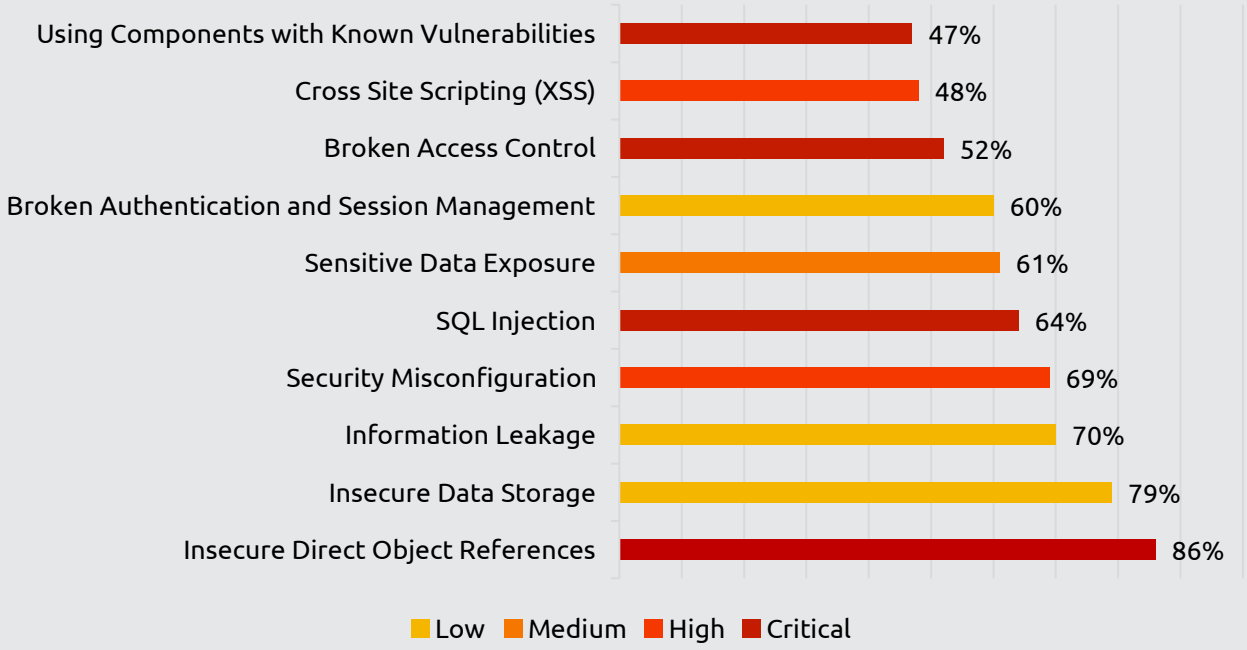
Tipos de Vulnerabilidades mais Resolvidas em 2020



Relativamente aos tipos de vulnerabilidades mais resolvidas em 2020, verifica-se que existem 2 orientações que levam à resolução: a quantidade de vulnerabilidades e a sua severidade. No gráfico pode-se verificar que neste top 5 de resolução se encontram as vulnerabilidades mais comuns no global (Sensitive Data Exposure e Security Misconfiguration) e também as mais comuns no universo das críticas (XSS, Broken Access Control).

Tempos de Vida

Tempo de Vida para as 10 Vulnerabilidades mais resolvidas em 2020



O tempo de vida da vulnerabilidade consiste na 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.

Pode-se constatar que o tempo de vida é mais reduzido para as vulnerabilidades publicamente conhecidas em produtos off-the-shelf cujo patch de segurança já existe (Using Components With Known Vulnerabilities). No extremo oposto, é mais longo em situações que requerem desenvolvimento e redesenho da aplicação (Insecure Direct Object References).

As medianas de fecho refletem uma melhoria nos tempos de resolução para as vulnerabilidades Critical e High face ao ano de 2019, provavelmente devido a melhoria de processos de resolução para os clientes mais antigos.

Severidade	2015	2016	2017	2018	2019	2020	
Critical	13	34	49	41	39	33	↓
High	43	42	69	44	45	36	↓
Medium	48	67	47	56	45	52	↑
Low	51	35	58	48	40	55	↑

Mediana relativamente ao fecho por severidade.

Conclusão

Top Vulnerabilidades e Recomendações

A **Segurança da Informação** é um tema e uma realidade cada vez mais determinante e que não pode, de todo, ser relegada para segundo plano. É um aspeto crucial na gestão de negócios já que, em última instância, assegura e garante a segurança da informação – o maior ativo das organizações - contra potenciais incidentes ou ataques de segurança.

O risco tem de ser gerido e é importante que os clientes tenham noção das ameaças a que estão expostos diariamente. É um trabalho que tem de ser feito de forma continuada, uma vez que existem muitas vulnerabilidades, estando constantemente a aparecer novas.

Devido ao facto de introduzirem riscos, as mudanças têm elas próprias de ser acompanhadas de verificações, através do **Pentesting**, que é a única forma de garantir que os controlos são bem implementados. Customizado de acordo com as necessidades e objetivos de cada cliente, o Pentesting pode ser mais orientado para a componente técnica, para os processos, pessoas ou âmbitos combinados mais globais, dependendo daquilo que o cliente pretende e precisa.

Tal como referido ao longo do relatório, a prática da INTEGRITY de Auditoria em cibersegurança auxilia os clientes a identificarem potenciais riscos, nomeadamente vulnerabilidades técnicas através da realização de Testes de Intrusão Pontuais ou Persistentes - **KEEP-IT-SECURE-24**- providencia recomendações e suporte para a mitigação das questões identificadas. O KEEP-IT-SECURE-24 apresenta-se como uma nova abordagem na redução efetiva do risco, suportando o escalonamento, a monitorização, a comunicação e as métricas das vulnerabilidades.

Em relação aos três grandes setores analisados - setor Financeiro, setor da Indústria & Energia e setor dos Serviços - constatou-se, através da análise dos gráficos, que se encontram todos nivelados quanto às práticas de cibersegurança, contudo verifica-se no Financeiro maior eficácia na resolução e nos Serviços maior eficiência no processo.

Outro ponto importante a reter, é a natureza permanente das vulnerabilidades, já que há forças que levam a que não exista, de facto, estabilidade a este nível.

Com o tempo, é natural que surjam cada vez mais vulnerabilidades, potenciadas por desatualização do software e dos sistemas; mudanças nas infraestruturas e nas aplicações, que podem induzir a novas falhas; os novos assets já que quanto mais componentes são adicionados a infraestruturas mais probabilidade há de haver vulnerabilidades; falta de sensibilização das pessoas nos temas da segurança e, por fim, no caso particular da INTEGRITY a profundidade dos seus testes faz com que haja algum espaço de serem descobertas vulnerabilidades ao longo do tempo que num Pentest tradicional não seriam.

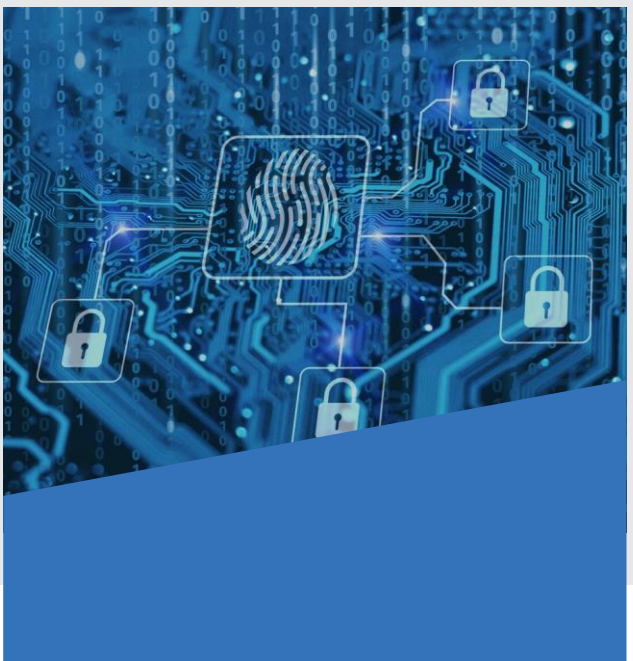
Os **comportamentos dos indivíduos** também são uma vertente essencial das boas práticas de cibersegurança. A educação e a sensibilização para a adoção de atitudes e comportamentos mais adequados para uma maior proteção dos indivíduos e das organizações são pontos basilares, já que muitas das vulnerabilidades identificadas têm a ver com a falta de sensibilização de quem se envolve, configura e gere os sistemas.

De acordo com o Relatório Cibersegurança em Portugal – Sociedade 2020 do Centro Nacional de Cibersegurança (CNCS), a componente educacional e de sensibilização tem vindo a ganhar robustez, mostrando indicadores mais favoráveis. O que é, sem dúvida, positivo.

Ao olhar para a média da União Europeia em comparação com Portugal, é notório que os indivíduos e as organizações nacionais ainda não adotam comportamentos suficientemente adequados para a melhor proteção possível contra as ameaças do ciberespaço, no entanto apesar desta evidência, a tendência anual é, em parte, positiva.

Quanto às **recomendações**, há um conjunto de boas práticas e orientações que as empresas e indivíduos devem adotar e ter em conta. Para além das já referidas no documento, ao nível das SSL/TLS deve-se **definir "checklists"** de configuração e **garantir a desabilitação de protocolos** obsoletos ou pouco seguros. Os **updates**, que consistem na verificação regular e atenta das atualizações devem ser feitos e, no caso de haver vulnerabilidades do tipo Critical, aconselha-se a serem implementados **processos de atualização rápida**.

Em suma, a resposta para mitigar o crescimento dos ataques – que devem e têm de ser encarados como um problema de negócio – tem de passar não só pelo reforço da utilização de soluções tecnológicas mas também pela implementação de processos e aposta em serviços de excelência que ajudem efetivamente as organizações a detetar, de forma antecipada, as ameaças, combater de forma eficaz os ataques, estando sempre em alerta, perante alterações ou comportamentos "anormais" ou de risco, manter os sistemas atualizados, efetuar ações de Pentesting para antecipar potenciais riscos e criar processos bem estabelecidos para a gestão da segurança.



A evolução constante das ameaças – tal como demonstraram os gráficos analisados - e a dinâmica da tecnologia da informação obriga a uma constante adaptação das práticas, ferramentas e abordagens na área da cibersegurança.

Capitalizando a experiência, know-how e reconhecimento das necessidades de cada cliente, a INTEGRITY tem no seu ADN a criação continuada de abordagens inovadoras de valor acrescentado, podendo efetivamente ajudar de forma assertiva no combate a possíveis ataques de segurança.

Privilegiar as soluções descentralizadas, com especial ênfase na identidade em vez da localização é, mais do que nunca, uma prioridade uma vez que a necessidade de acesso dos utilizadores a dados, em qualquer lado e a qualquer hora, foi potenciada com a pandemia assim como a obrigatoriedade de teletrabalho e será certamente tendência a manter. Neste cenário, a utilização de boas políticas de password em conjugação com Multi Factor Authentication torna-se vital.

INTEGRITY S.A.

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
Suite 4B43 Berkeley Square
Mayfair, Westminster
London, W1J 5FJ | United Kingdom

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

www.integrity.pt
www.keepitsecure24.com

INTEGRITY
Part of Devoteam

KEEP IT SECURE 24