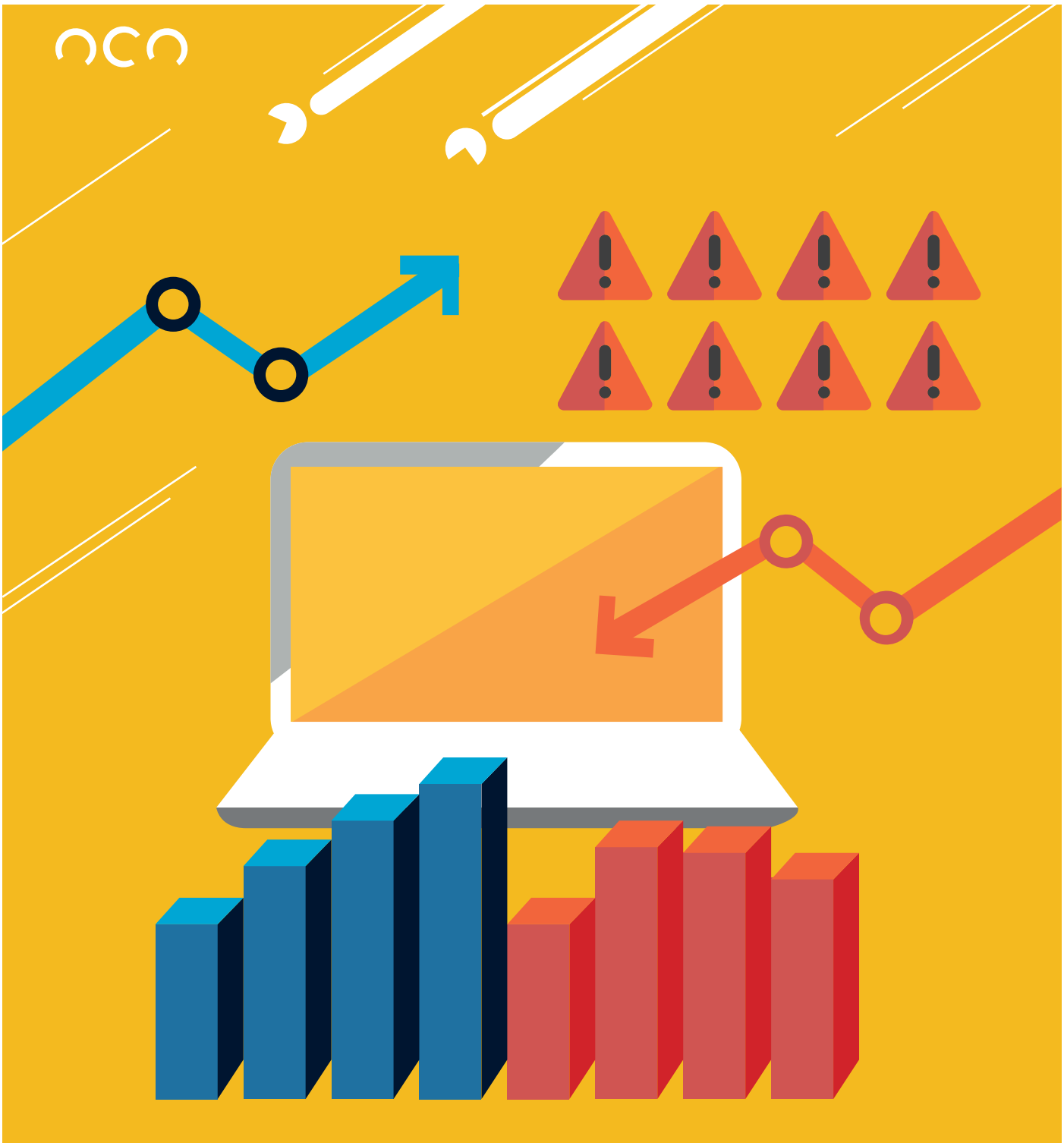
iBLISS

Relatório de Ameaças de 2016



SUMÁRIO

iBLISS

PARTE 1: INTRODUÇÃO

A iBLISS apresenta o *Relatório de Ameaças 2016*, feito com base em sua larga experiência em cibersegurança, acumulada ao longo de anos de investimento em pesquisa, desenvolvimento, observação e análise dos ambientes de segurança de empresas pertencentes a mercados diversos.

O estudo teve como base pesquisas realizadas em mais de 70 empresas de diversos setores, incluindo cartões, esportes, e-commerce, finanças, indústria, internet, logística, seguros, tecnologia, telecomunicações e varejo. A pesquisa incluiu dados dos últimos 12 meses e abordou vulnerabilidades de infraestrutura e aplicações web para traçar um panorama das principais falhas de segurança encontradas nas empresas brasileiras e suas dificuldades na gestão de ameaças e vulnerabilidades.

Foram encontradas, ao todo, quase 18.500 vulnerabilidades, das quais **20% são críticas e de alta criticidade**. Falhas como essas representam a maior ameaça, pois, se forem exploradas, causarão os maiores danos ao negócio. Além disso, **quase metade das vulnerabilidades (49%) foi classificada como de média criticidade**, gerando um cenário de **69% de falhas que tem impacto relevante** e podem causar danos significativos aos negócios.

No processo, a iBLISS fez uso do GAT, uma plataforma inovadora com tecnologia desenvolvida no Brasil, capaz de oferecer gestão de vulnerabilidades de forma integrada, centralizando informações de diversas ferramentas de escaneamento em uma única interface.

A pesquisa permitiu criar um relatório inédito para guiar os tomadores de decisão em suas estratégias de segurança, gestão de vulnerabilidades e remediação.

Sobre a pesquisa de ameaças desenvolvida pela iBLISS

O *Relatório de Ameaças 2016* leva em consideração vulnerabilidades de infraestrutura e vulnerabilidades de aplicações, classificadas de acordo com o grau de criticidade em quatro níveis: críticas, alta criticidade, média criticidade e baixa criticidade.

As categorias de classificação usadas foram: **Acesso Remoto, Desatualização, Gerenciamento de Configuração, Gerenciamento de Sessão, Gerenciamento de Usuários, Protocolo Inseguro, Levantamento de Informações, Teste de Autenticação, Teste de Autorização, Validação de Dados, Negação de Serviço e Lógica de Negócios.**

Confira o significado dos principais conceitos usados:

AMEAÇA

Esse termo é extremamente abrangente e corresponde à origem ou à intenção de executar um ataque. Os testes de invasão, por exemplo, são focados em avaliar perfis de ameaças para ajudar as empresas a estabelecer medidas de remediação contra os ataques representados por ameaças específicas.

VULNERABILIDADE

Refere-se a falhas de segurança na infraestrutura ou em aplicações que permitem que os ataques sejam bem-sucedidos. O processo de identificação de vulnerabilidades deve ser contínuo nas empresas para que os profissionais de segurança possam responder efetivamente a cada uma delas antes que um ataque ocorra.

RISCO

O termo risco corresponde à probabilidade de sofrer um determinado ataque e de que ele seja bem sucedido. Por isso, um risk assessment, muito além de enumerar potenciais ataques, ajuda a determinar quais são os pontos que precisam de mais atenção de acordo com o custo de um possível ataque (que varia de acordo com a criticidade dos sistemas atingidos) e sua probabilidade.

VULNERABILIDADES DE ESTRUTURA

São as vulnerabilidades encontradas em toda a infraestrutura de TI, incluindo a rede e suas configurações, como servidores, estações de trabalho e equipamentos de rede, a atualização e as configurações de softwares usados nos processos de negócio e a gestão do acesso aos dados críticos por funcionários.

VULNERABILIDADES DE APLICAÇÃO

Refere-se às vulnerabilidades em aplicações web, que correspondem a bugs e falhas de segurança em aplicações web, apps e serviços que permitem problemas como ataques de negação de serviço (DDoS), levantamento de informações da infraestrutura e acesso restrito aos sistemas e programas.

VULNERABILIDADES CRÍTICAS

São vulnerabilidades cuja exploração pode levar ao comprometimento em larga escala da infraestrutura de TI. São brechas facilmente exploradas, pois o hacker não precisa de nenhuma credencial especial e nem precisa persuadir um usuário. Esse tipo de falha precisa ser remediado o mais rápido possível.

VULNERABILIDADES DE ALTA CRITICIDADE

Geralmente são de mais difícil exploração, mas podem levar a problemas como elevação de privilégios, perda de dados e downtime.

VULNERABILIDADES DE MÉDIA CRITICIDADE

São vulnerabilidades que requerem que o criminoso manipule as vítimas, portanto são mais trabalhosas para o hacker. Essas falhas geralmente exigem que o cibercriminoso tenha privilégios de usuário.

VULNERABILIDADES DE BAIXA CRITICIDADE

Causam impacto muito baixo nos negócios, pois exigem que o cibercriminoso tenha acesso físico ou local ao sistema. Por serem menos perigosas, podem ser preteridas.

Resumo dos principais insights do relatório

O *Relatório de Ameaças 2016* confirma as dificuldades das empresas brasileiras com a gestão de vulnerabilidades. Ainda é considerável o número de falhas de segurança graves que podem ser facilmente resolvidas, mas que, por causa de desafios na gestão, seguem sem solução.

Um exemplo disso são as falhas de atualização de sistemas, que foram as vulnerabilidades críticas mais comuns encontradas nas empresas brasileiras, respondendo por **92% das falhas de segurança críticas de infraestrutura**. Um único software desatualizado pode levar ao comprometimento em larga escala da infraestrutura de TI.

O estudo mostrou ainda que **5% das vulnerabilidades envolvendo desatualização de sistemas** correspondem a falhas de OpenSSL que permitem o acesso a informações sensíveis por meio de bugs diretamente ligados ao **Heartbleed**, uma falha de segurança já divulgada desde 2014.

92%
Desatualização

5% das vulnerabilidades envolvendo desatualização de sistemas correspondem a bugs diretamente ligados ao Heartbleed

De acordo com o estudo, **as vulnerabilidades críticas, de alta criticidade e de média criticidade são 69% das falhas de segurança brasileiras**. Esse número pode ser considerado alto, ainda que a maioria das falhas de segurança desse grupo sejam as de média criticidade (**que correspondem a 49% das vulnerabilidades encontradas**).

Isso porque, mesmo que sejam vulnerabilidades menos graves e de mais difícil exploração, em um ataque persistente avançado, por exemplo, que conta com hackers com maior nível de expertise e paciência para atingirem seu objetivo, os impactos para o negócio podem ser significativos. No caso das vulnerabilidades de baixa criticidade, mesmo que sejam exploradas, o impacto para o negócio é considerado baixo.

Entre as falhas de alta criticidade, por exemplo, **61% correspondem a vulnerabilidades que permitem o acesso remoto à rede, erro que pode levar ao roubo de dados e à paralisação de processos fundamentais.**

Concluímos, portanto, que quase **70% das vulnerabilidades encontradas nos últimos 12 meses podem causar danos significativos ao negócio.**

69%
Vulnerabilidades críticas de alta e média criticidade

61% das vulnerabilidades de alta criticidade permitem o acesso remoto à rede

Quase 70% das vulnerabilidades encontradas nos últimos 12 meses podem causar danos significativos ao negócio

Setor financeiro é o que conta com a maior porcentagem de falhas de segurança críticas

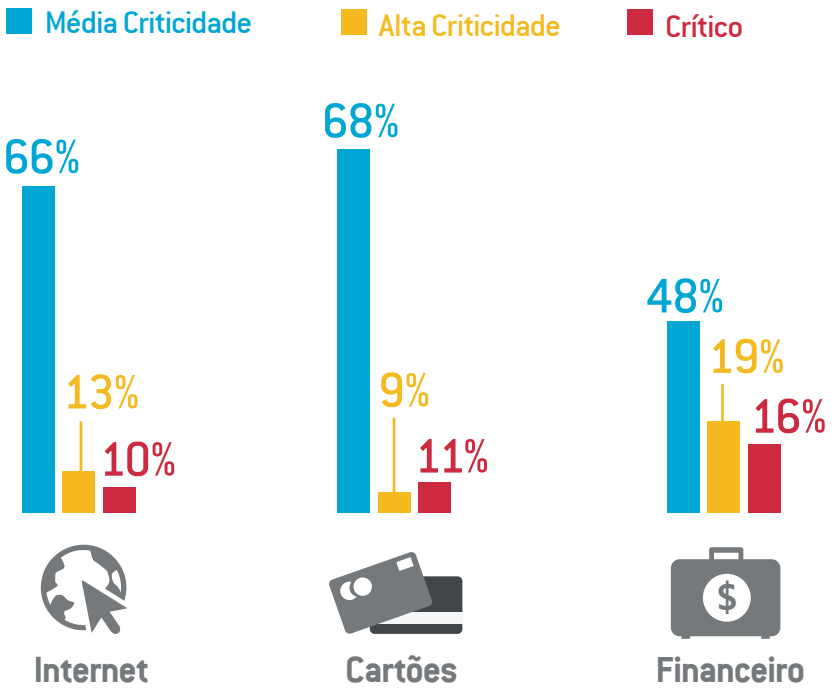
Os setores mais vulneráveis

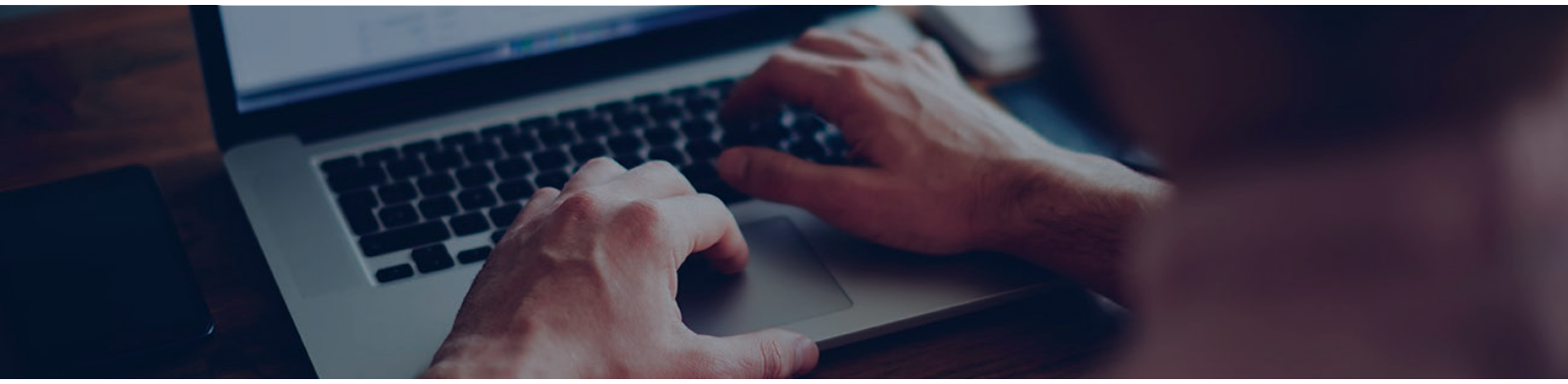
O *Relatório de Ameaças 2016* mostra uma proporção muito maior de vulnerabilidades críticas, de alta criticidade e média criticidade nos setores financeiro, de cartões e de internet. No caso do setor financeiro, **esse grupo de vulnerabilidades responde por 83%**, enquanto **no setor de cartões esse número sobe para 88%** e, **no setor de internet, fica em 89%**.

No caso do setor financeiro, **a porcentagem de vulnerabilidades críticas é a mais alta de todos os setores analisados, chegando a 16%**. Vale lembrar que o setor é um dos que mais investem em segurança no Brasil. Os números do relatório mostram, portanto, que a tendência é que cada vez mais investimentos sejam feitos na área para tornar o negócio mais rentável e seguro.

O setor de internet se destaca pelas vulnerabilidades de média criticidade, especialmente as falhas de configuração em aplicações web.

Setores mais vulneráveis: Vulnerabilidades críticas, de alta e média criticidade





PARTE 2: PRINCIPAIS RESULTADOS DA PESQUISA

Quantidade de IPs analisada nas empresas brasileiras é muito maior que a quantidade de aplicações analisadas

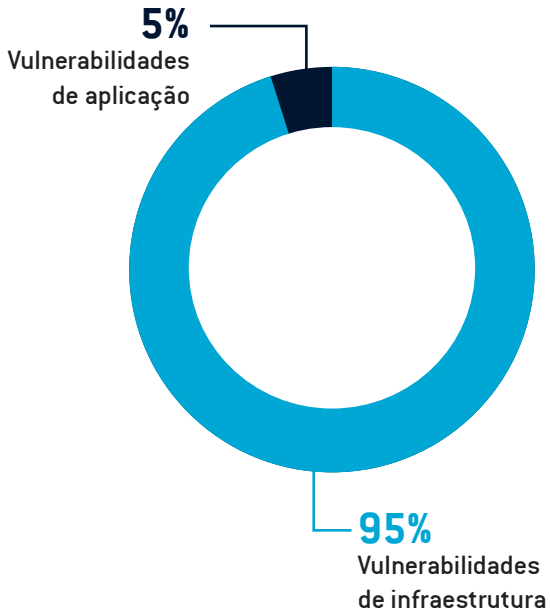
Nesta seção, encontram-se as principais descobertas deste estudo. Os tópicos são apresentados na seguinte ordem:

Vulnerabilidades de infraestrutura

Vulnerabilidades de aplicação

Vulnerabilidades por setor

Setores mais vulneráveis: Vulnerabilidades críticas, de alta e média criticidade



O Gráfico 1 a seguir mostra a proporção das vulnerabilidades dos últimos 12 meses de acordo com a área em que foram encontradas:

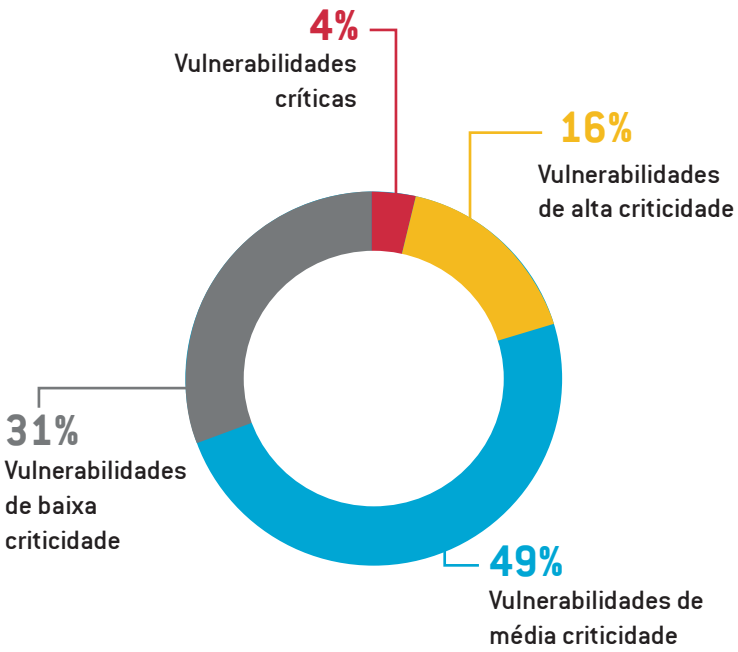
As vulnerabilidades de infraestrutura respondem pela maioria dos problemas encontrados, representando 95% das brechas de segurança identificadas nos últimos 12 meses, enquanto **as vulnerabilidades de aplicação correspondem a apenas 5% dos resultados**.

Isso acontece porque a quantidade de IPs analisados nas empresas brasileiras geralmente é muito maior que a quantidade de aplicações analisadas. Algo que se deve a um foco do mercado nacional em testes de infraestrutura (Pentest Blackbox) em detrimento dos testes de aplicação web.

O estudo também mostrou que, apesar de estarem em menor número, **as vulnerabilidades de aplicação têm maior incidência de vulnerabilidades críticas, chegando a 11%**, enquanto apenas **4% das vulnerabilidades de infraestrutura foram consideradas críticas.**

20% dos problemas encontrados correspondem a falhas críticas e de alta criticidade

Vulnerabilidades por criticidade



O Gráfico 2 mostra a proporção total de vulnerabilidades (de infraestrutura e de aplicações) de acordo com sua criticidade:

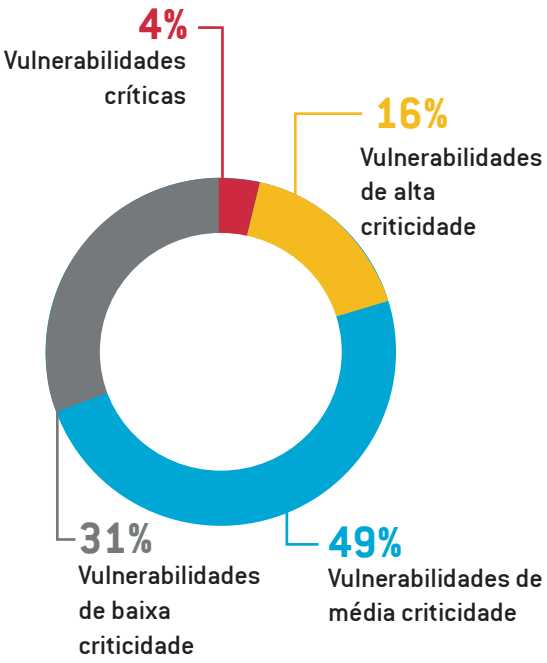
Quase metade dos problemas encontrados (49%) correspondem a vulnerabilidades de média criticidade, enquanto as **vulnerabilidades críticas, que exigem remediação imediata, responderam por apenas 4% das vulnerabilidades encontradas**.

Vulnerabilidades de baixa criticidade respondem por 31% das falhas, **ficando a frente das vulnerabilidades de alta criticidade (16%)**, que também exigem certa urgência em sua remediação.

Isso mostra que grande parte das vulnerabilidades encontradas (80%) não são facilmente explorada, porém **20% são responsáveis pelos mais graves problemas e exploradas pelos cibercriminosos**. Isso porque as vulnerabilidades de média criticidade requerem que os hackers tenham acesso de usuário para conseguir executar um ataque bem-sucedido, algo que pode ser obtido por meio de múltiplas tentativas por parte do cibercriminoso e gerar também grandes prejuízos para a empresa.

No caso das vulnerabilidades de baixa criticidade, o grau de dificuldade para os cibercriminosos é ainda maior e essas falhas geralmente têm baixo impacto para o negócio caso sejam usadas para executar um ataque.

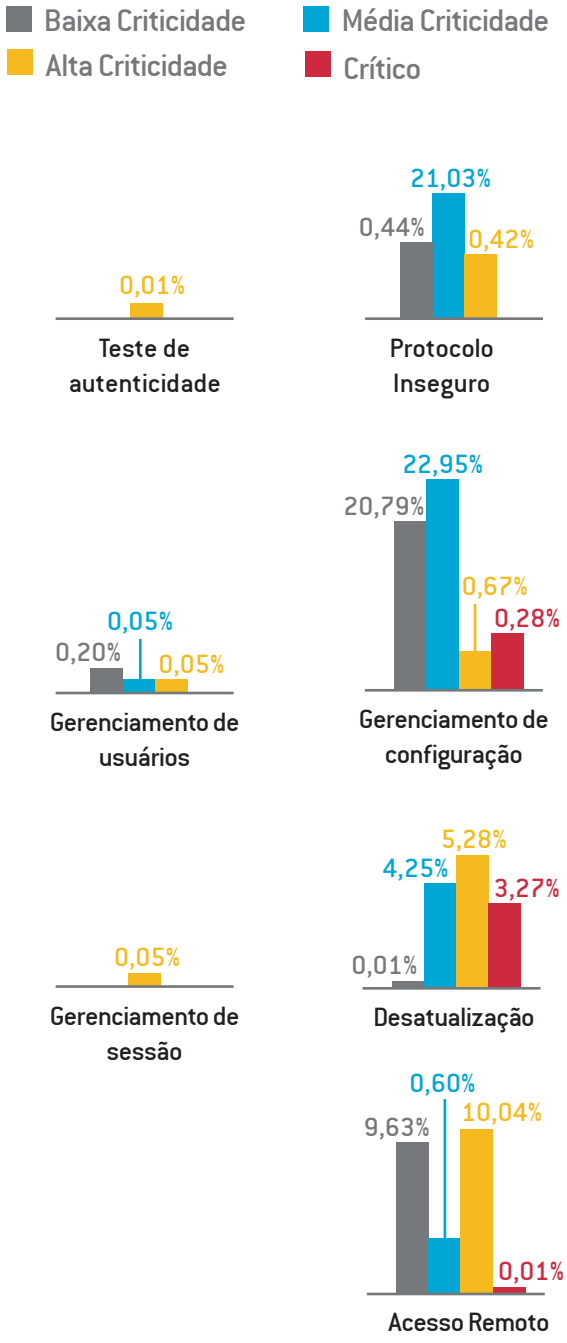
Vulnerabilidades de infraestrutura



Os Gráficos 3 e 4 exibem os tipos de vulnerabilidades encontrados em cada nível de criticidade e a proporção das vulnerabilidades de infraestrutura (**95% das vulnerabilidades identificadas nos últimos 12 meses**) de acordo com seu grau de criticidade:

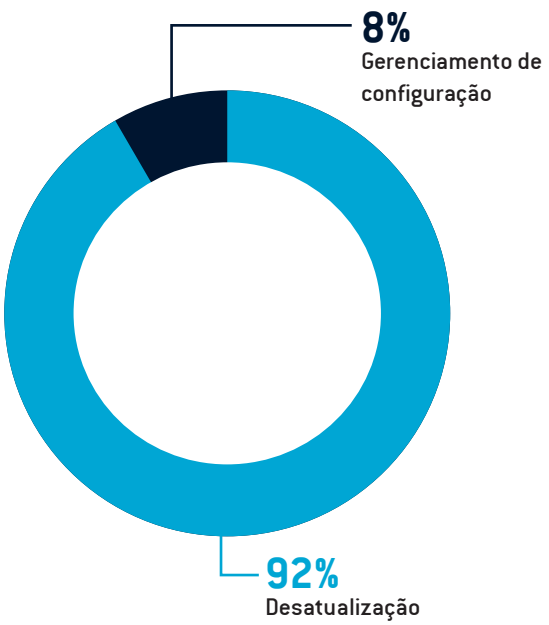
O estudo mostra que as falhas de segurança de média criticidade também correspondem à maioria das vulnerabilidades de infraestrutura encontradas nas empresas. Em segundo lugar, ficam **as vulnerabilidades de baixa criticidade (31%),** seguidas pelas de **alta criticidade (16%)** e as **críticas (4%).**

Consolidado das vulnerabilidades de infraestrutura



Vulnerabilidades críticas

Maioria das falhas críticas está relacionada à ausência de pacotes de atualização



O Gráfico 5 a seguir mostra a proporção das classificações das vulnerabilidades críticas de infraestrutura encontradas em 2016:

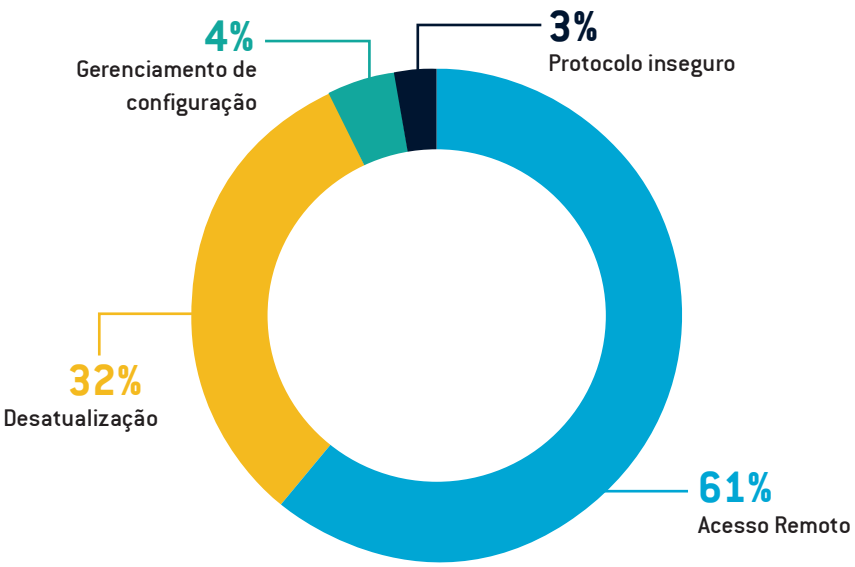
Entre as **vulnerabilidades críticas** de infraestrutura, **as que estão relacionadas à desatualização de sistemas respondem por 92%**. Segundo descobertas do estudo, a maioria das falhas diz respeito à ausência de pacotes de atualização críticos de aplicações como Apache, VMware e Windows ou ao uso de versões não suportadas pelo fabricante.

Isso é um indício de que as empresas ainda têm dificuldades na gestão de patches, permitindo que softwares vulneráveis sejam usados nos processos de negócio. Vale lembrar que as vulnerabilidades críticas precisam de remediação imediata, pois são facilmente exploradas por cibercriminosos e podem causar sérios danos aos sistemas, gerando vazamentos de dados e perdas com downtime.

Vale destacar que as falhas críticas de segurança são exploradas de forma automatizada, transformando ambientes produtivos em servidores gerenciados para realização de ataques como DDoS.

As falhas de configuração, como problemas relacionados ao uso de credenciais, respondem por 8% das falhas críticas de infraestrutura.

Vulnerabilidades de alta criticidade



No Gráfico 6 abaixo, é possível observar a proporção das classificações de vulnerabilidades consideradas de alta criticidade.

Problema do Heartbleed ainda não foi resolvido

Uma das descobertas do estudo é a de que **5% das vulnerabilidades de desatualização de alta criticidade correspondem a falhas de OpenSSL,** que permitem o acesso a informações sensíveis por meio de bugs diretamente ligados ao **Heartbleed**.

O Heartbleed é uma falha na biblioteca de criptografia OpenSSL que foi divulgada amplamente em 2014. Como mostra o estudo, o problema continua deixando dados corporativos e de clientes vulneráveis, mesmo mais de um ano após a identificação da vulnerabilidade.

De acordo com o estudo, **as falhas de segurança que deixam a infraestrutura vulnerável ao acesso remoto são a maioria (61%) das vulnerabilidades de alta criticidade** – que não são tão facilmente exploradas, mas precisam de remediação rápida devido às consequências de um ataque, caso sejam exploradas.

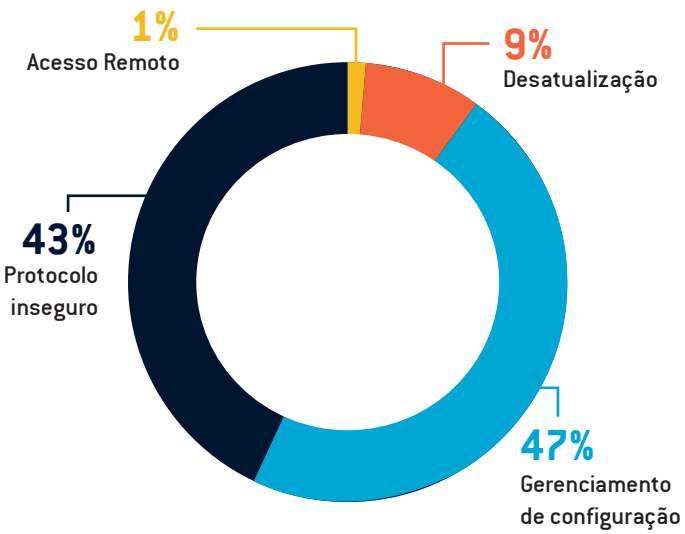
Entre as vulnerabilidades que deixam a rede exposta a acessos remotos, a mais encontrada foi por meio do **Remote Desktop Protocol (RDP), que responde por 36% das falhas de segurança com essa classificação**. Em seguida, **aparece o uso do protocolo SSH, que responde por 29% das vulnerabilidades** que possibilitam acesso remoto.

Como mostram os resultados do estudo, as vulnerabilidades de atualização se destacam também entre as de alta criticidade, evidenciando a dificuldade das empresas com a gestão das atualizações.

Esse tipo de falha corresponde a 32% das vulnerabilidades de alta criticidade, com problemas como a ausência de pacotes de atualização importantes ou críticos e a execução de versões de programas que não possuem mais suporte dos fabricantes – **erros do tipo respondem por 44% das vulnerabilidades de desatualização de alta criticidade.**

Vulnerabilidades de média criticidade

Falhas relacionadas ao protocolo SSL são destaque entre as vulnerabilidades de alta criticidade



O Gráfico 7 mostra a proporção de vulnerabilidades de média criticidade de acordo com sua classificação:

As **vulnerabilidades de média criticidade** respondem pela maior parte das vulnerabilidades de infraestrutura e se diferenciam por não serem de fácil exploração, pois requerem que os cibercriminosos manipulem suas vítimas para obter acesso privilegiado.

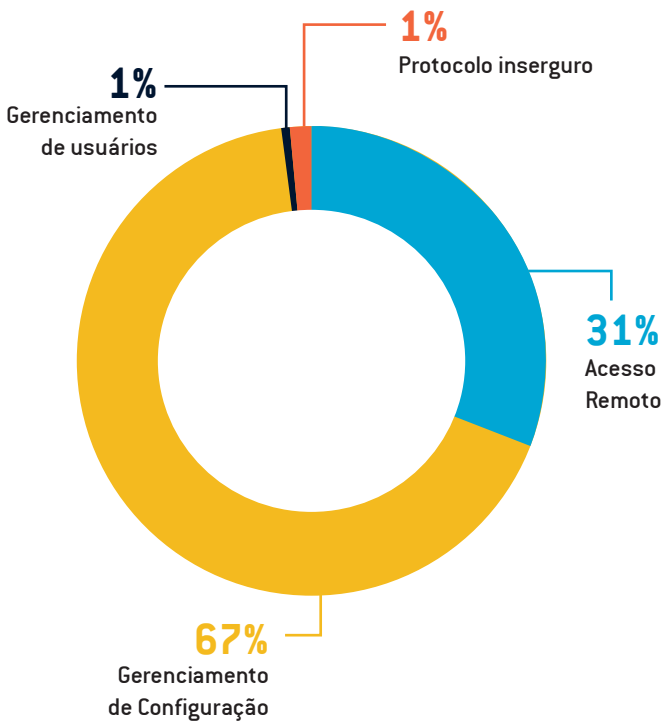
Nessa classificação se destacaram no estudo **as vulnerabilidades relacionadas a protocolos inseguros (43%)** e **falhas de configuração (47%)**. As vulnerabilidades relacionadas à **desatualização de softwares respondem por apenas 9%** das vulnerabilidades de média criticidade.

O OpenSSL também se destaca como origem de vulnerabilidades de média criticidade. Segundo o estudo, em **37% das vulnerabilidades de gerenciamento de configuração de média criticidade,** o OpenSSL estava vulnerável a vazamentos de informações sensíveis, desta vez, com relação ao **POODLE**, um ataque do tipo *man-in-the-middle*, em que um hacker se coloca no meio de uma comunicação com o objetivo de ter acesso aos dados trafegados. O POODLE (descoberto também em 2014) tira vantagem da versão 3.0 do SSL.

Os dados relacionados às falhas de protocolos inseguros também dão destaque ao SSL. **Em 56% das vulnerabilidades com essa classificação**, o servidor estava utilizando chaves criptográficas inadequadas para o protocolo SSL/TLS e, **em 31% delas, foram encontrados certificados SSL assinados por uma Autoridade Certificadora desconhecida**.

O SSL é amplamente utilizado em diversas empresas na criptografia das comunicações, no entanto, são muitas as falhas do protocolo às quais as empresas devem ficar atentas. Além das vulnerabilidades mais comuns já citadas, **4% das vulnerabilidades de protocolo inseguro correspondem a certificados SSL expirados**.

Vulnerabilidades de baixa criticidade



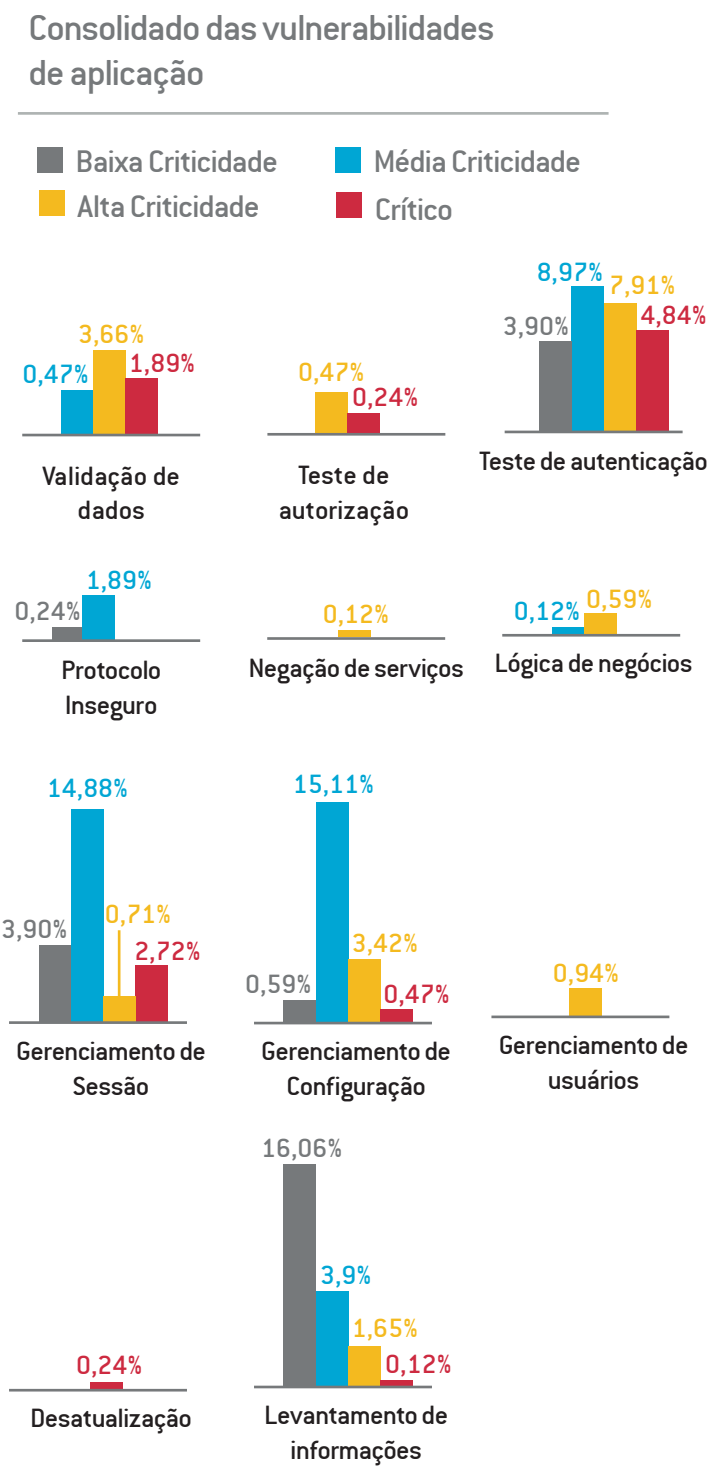
O Gráfico 8 mostra a proporção das vulnerabilidades de baixa criticidade de acordo com sua classificação. **As vulnerabilidades de baixa criticidade correspondem a 31% das vulnerabilidades de infraestrutura.**

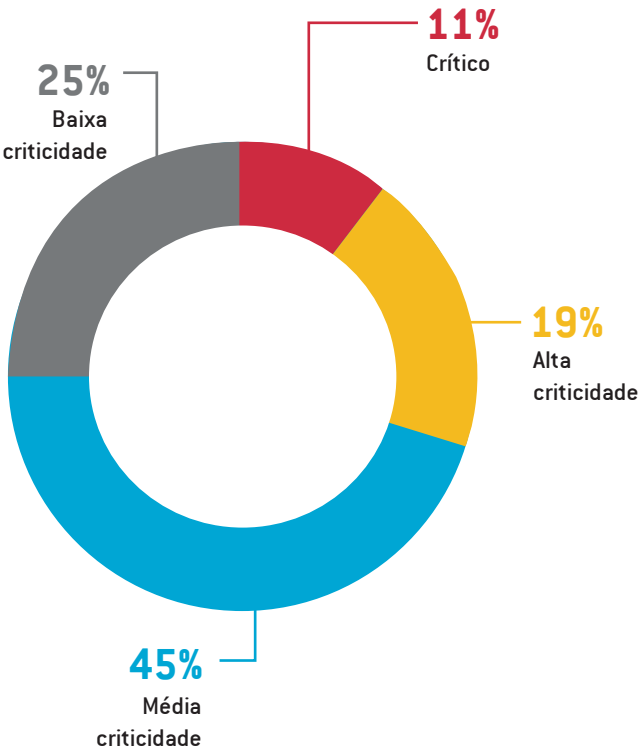
O estudo mostra que **as falhas de segurança de baixa criticidade são, em sua maioria, falhas de configuração (67%)**. Dentre os erros mais encontrados na gestão de configurações, **23% são falhas no Microsoft Windows SMB que permitem o vazamento de informações de sistemas remotos.**

Vulnerabilidades de baixa criticidade necessitam de menos atenção por parte dos profissionais de segurança por causa de seu baixo impacto nos negócios.

Maioria das vulnerabilidades de baixa criticidade são falhas de configuração (**67%**)

Vulnerabilidades de aplicação



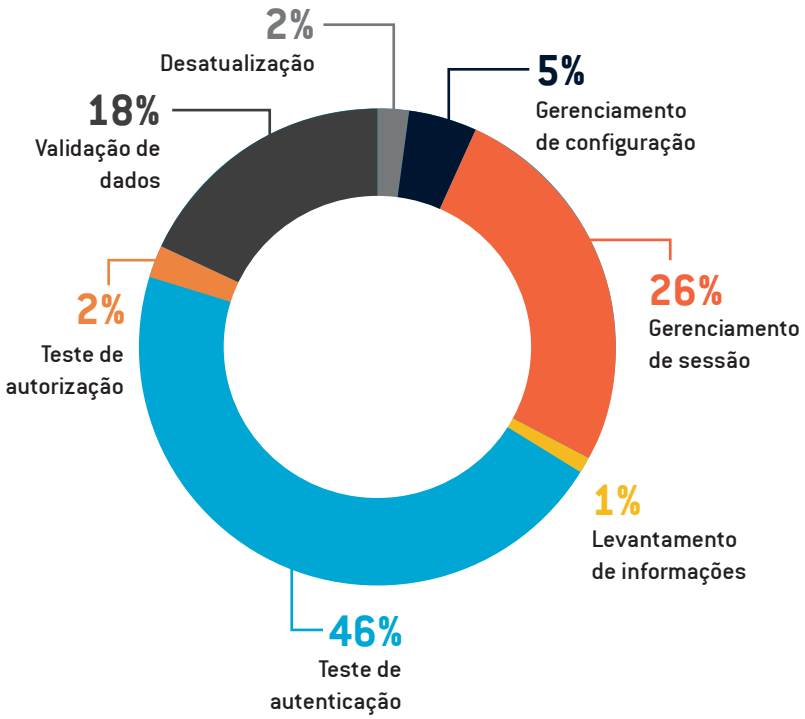


Os Gráficos 9 e 10 reúnem dados do estudo que permitem observar a proporção das vulnerabilidades de aplicação de acordo com sua categoria e criticidade.

Observa-se que a proporção das vulnerabilidades críticas e de alta criticidade é maior nas falhas de segurança de aplicação do que nas brechas de infraestrutura.

Juntas, **as vulnerabilidades críticas e de alta criticidade correspondem a 30% das brechas de aplicação**, enquanto, **nas de infraestrutura, a proporção é de 20%**.

Vulnerabilidades críticas



O Gráfico 11 mostra a proporção das vulnerabilidades críticas de aplicação de acordo com sua classificação no estudo.

Falhas de autenticação, como permissão de acesso anônimo, são a maioria das vulnerabilidades críticas de aplicação

Segundo o estudo, **entre as vulnerabilidade críticas se destacam as falhas de autenticação (46%)**, em que a mais comum é a ausência de TLS e a permissão de acesso anônimo.

O TLS é um importante protocolo para garantir ao usuário que seus dados estejam criptografados.

Além das vulnerabilidades de teste de autenticação, destacam-se também as **falhas de gerenciamento de sessão (26%)**. Nesse tipo de brecha são comuns as vulnerabilidades de roubo de sessão e o gerenciamento inadequado, erros que podem dar a hackers acesso privilegiado a dados sigilosos.

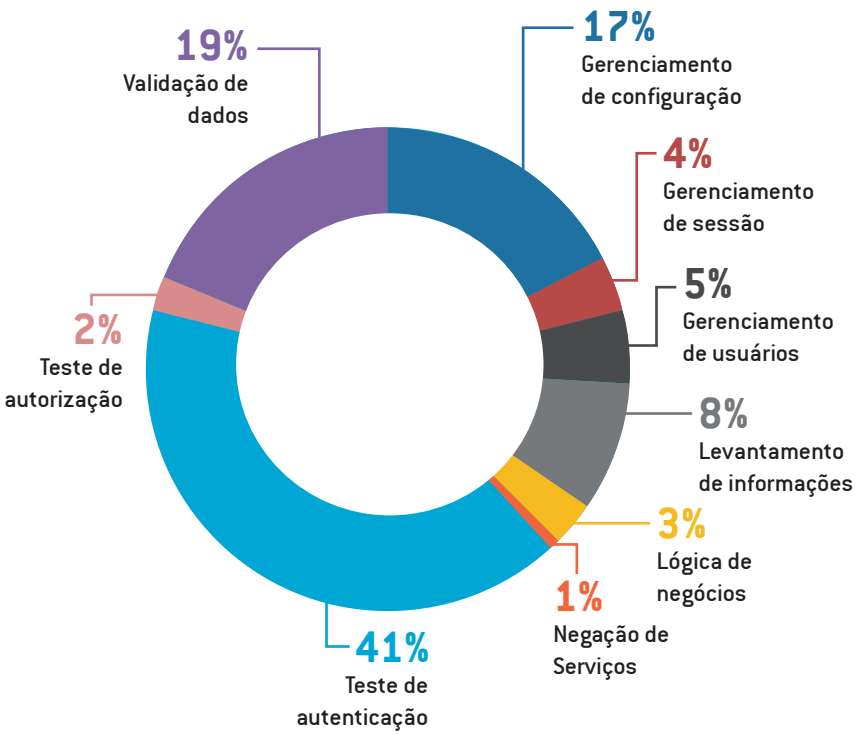
Vulnerabilidades de validação de dados respondem por 18% das vulnerabilidades críticas de aplicação web, incluindo injeções de SQL e permissão excessiva para upload.

De acordo com o estudo, **as falhas de gerenciamento de sessão (5% das vulnerabilidades críticas de aplicação)** está a exposição do código fonte.

Além disso, **2% dos erros críticos correspondem a falhas de desatualização** e **1% das brechas está relacionado ao levantamento de informações**.

Vulnerabilidades de alta criticidade

Testes de autenticação respondem pela maioria das vulnerabilidades de alta criticidade em aplicações

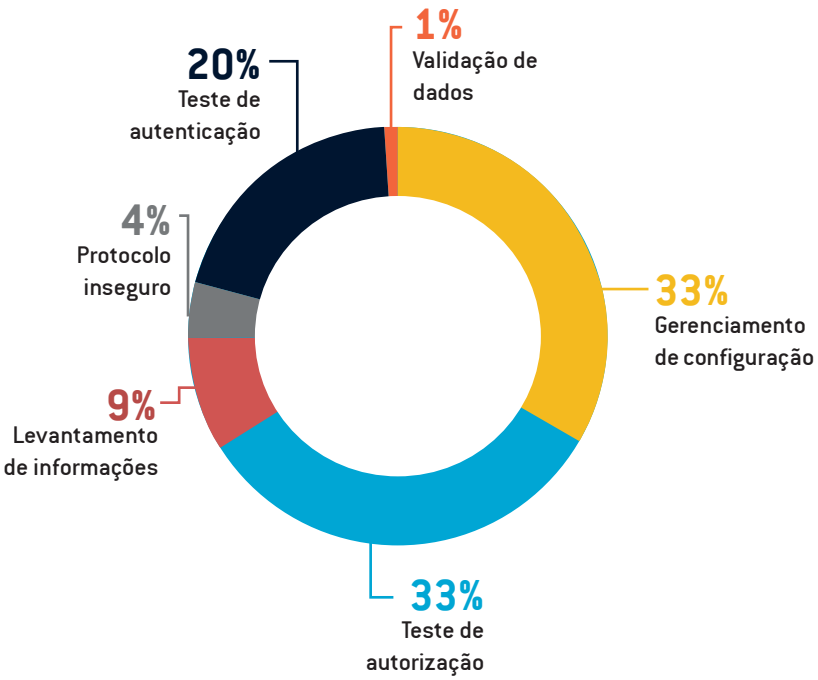


O Gráfico 12 exibe a proporção das vulnerabilidades de alta criticidade de acordo com sua classificação. **Esse tipo de falha responde por 19% das vulnerabilidades de aplicação**.

O estudo mostra que, entre as vulnerabilidades de alta criticidade envolvendo aplicações, **as que estão relacionadas aos testes de autenticação são as mais frequentes, respondendo por 41% das falhas de segurança identificadas.**

Nessa categoria, as mais comuns são a falta de criptografia de senhas e as aplicações acessíveis via HTTP, falhas características de um controle de acesso deficiente, em que pessoas não autorizadas podem facilmente ter acesso a dados importantes de aplicações web, colocando os negócios em risco.

Vulnerabilidades de média criticidade



Maioria das vulnerabilidades em aplicações são de média criticidade

O Gráfico 13 exibe as vulnerabilidades de aplicação de média criticidade de acordo com sua classificação. **Essas falhas são a maioria das falhas de segurança dessa área, respondendo por 45% das vulnerabilidades encontradas no estudo.**

As vulnerabilidades de média criticidade em aplicações, assim como em infraestrutura, são a maioria das falhas identificadas. Nesse nível de gravidade, de acordo com os dados analisados, **os erros de gerenciamento de sessão são a maioria (33%)**, seguidos pelos **erros de configuração (33%)**.

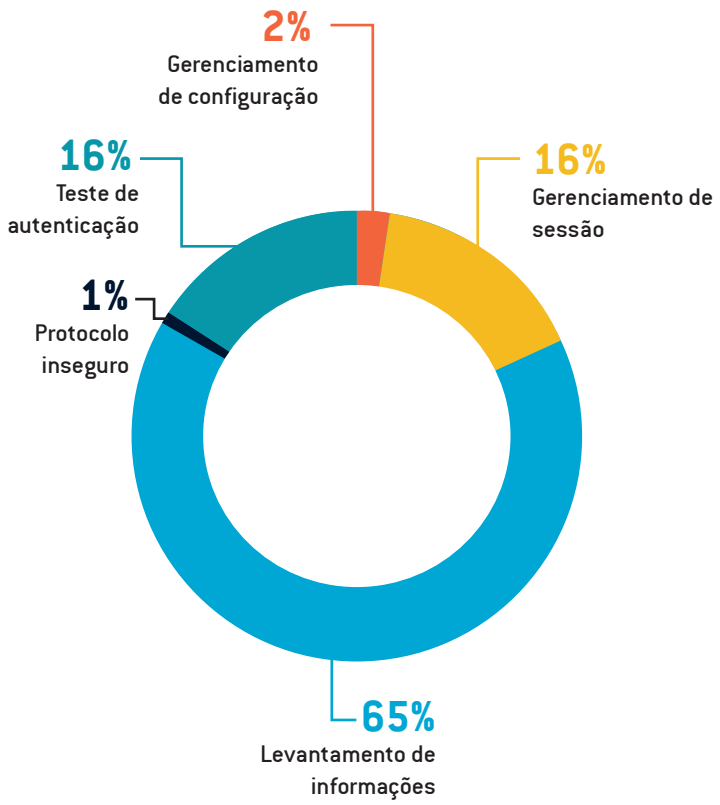
Entre os erros de gerenciamento de sessão destacam-se as falhas relacionadas a cookies, como a ausência do atributo HTTP Only e Secure.

O atributo HTTP Only sinaliza para o navegador que apenas o servidor pode ter acesso ao cookie que leva essa tag. Qualquer tentativa de acessar cookies de clientes, logo, é bloqueada. Isso é essencial para impedir que servidores remotos maliciosos tenham acesso a informações pessoais.

O atributo Secure tem uma função semelhante, evitando que os cookies sejam observados por indivíduos maliciosos. Quando os cookies levam essa característica, os browsers só atendem a solicitações para páginas HTTPS, pois o navegador não envia esse tipo de cookie sem criptografia.

Essas configurações são essenciais para evitar vazamentos de dados e, consequentemente, danos financeiros ao negócio e à reputação da empresa.

Vulnerabilidades de baixa criticidade



O Gráfico 14 mostra a proporção das vulnerabilidades de aplicação de baixa criticidade, que correspondem a **25% das falhas de segurança de aplicação encontradas**.

De acordo com o estudo, a maioria das vulnerabilidades de baixa criticidade corresponde ao levantamento de informações. Ou seja, falhas que permitem aos hackers identificar aspectos chave da estrutura de aplicação web, como **a identificação de versões de serviços e tecnologias usadas (61%)**, **utilização incorreta de arquivos robots.txt e outros conteúdos publicados indevidamente (19%)** e a **descoberta de diretórios do servidor (9%).**

Ameaças de 2016 por setor

O *Relatório de Ameaças 2016* pesquisou mais de 70 empresas distribuídas entre os setores de **Cartões, E-Commerce, Esportes, Financeiro, Indústria, Internet, Logística, Seguros, Tecnologia, Telecomunicações e Varejo**. Todas as informações foram coletadas nos últimos 12 meses, e mostram quais são as vulnerabilidades mais comuns de cada setor, bem como a porcentagem de cada nível de criticidade em cada um deles.

O setor que mais registrou falhas de segurança foi o setor industrial, com 7.312 vulnerabilidades. As empresas desse segmento, no entanto, contam com poucas falhas de segurança críticas e com o maior número de vulnerabilidades de baixa criticidade.

A maior porcentagem de vulnerabilidades críticas fica com o setor financeiro, que, apesar de não ter contado com um alto número de falhas de segurança nos últimos 12 meses, conta com uma das maiores porcentagens de vulnerabilidades críticas, de alta e média criticidade, perdendo apenas para os setores de cartões e internet.

Ranking de setores por número de vulnerabilidades

1º Indústria
2º E-commerce
3º Internet
4º Seguros
5º Logística
6º Cartões
7º Financeiro
8º Telecomunicações
9º Esportes
10º Tecnologia
11º Varejo

Ranking de setores por porcentagem de vulnerabilidades críticas

1º Financeiro
2º Esportes
3º Telecomunicações
4º Cartões
5º Internet
6º Seguros
7º Tecnologia
8º Logística
9º E-commerce
10º Indústria
11º Varejo

Ranking de setores por porcentagem de vulnerabilidades críticas, de alta e média criticidade:

1º Internet
2º Cartões
3º Financeiro
4º Esportes
5º Telecomunicações
6º Seguros
7º Logística
8º E-commerce
9º Tecnologia
10º Varejo
11º Indústria

Desafios comuns a todos os setores

Segundo dados da pesquisa Cost of Data Breach Study 2016, do Instituto Ponemon, o Brasil está entre os países mais vulneráveis do mundo. O custo per capita de violação de dados no País cresceu de R$ 170,00 em 2014 para R$ 225,00 em 2015 e o prejuízo das empresas brasileiras passou de R$ 3,96 milhões para R$ 4,31 milhões no mesmo período.

Ainda de acordo com o estudo do instituto Ponemon, 30% das violações correspondem a funcionários ou organizações que negligenciaram a segurança de dados.

A gestão de vulnerabilidades é essencial para reduzir custos e riscos com cibersegurança e cada vez mais empresas brasileiras estão reconhecendo a importância de contar com estratégias para remediar falhas de segurança de acordo com sua criticidade, levando em consideração o contexto do negócio.

Todas as empresas têm vulnerabilidades, porém, é praticamente impossível solucionar cada uma delas. Isso é o que torna a gestão de vulnerabilidades um desafio para organizações de todos os setores. Um dos problemas mais encontrados é a falta de integração entre as diversas plataformas de segurança e auditoria, dificultando a capacidade das empresas de ter uma visão ampla e classificar as falhas de acordo com os riscos oferecidos.

Saiba mais sobre os principais desafios encontrados pelas empresas brasileiras na gestão de vulnerabilidades:

A maioria das empresas leva, em média, 103 dias para remediar uma vulnerabilidade

PRIORIZAÇÃO

A maioria das empresas brasileiras ainda não conta com um sistema para ajudar a **priorizar as vulnerabilidades** com base na importância de seus ativos e sua criticidade e acabam ficando com uma grande quantidade de dados que precisam ser geridos sem que haja um entendimento de **quais vulnerabilidades são realmente críticas para o negócio.**

Para vencer esse problema, as organizações precisam de contexto para obter uma visão holística do ambiente de TI.

REMEDIAÇÃO

A maioria das empresas leva, em média, 103 dias para remediar uma vulnerabilidade, criando uma grande oportunidade de ataque para os cibercriminosos. Isso acontece porque ainda faltam tecnologias capazes de resolver o problema efetivamente de maneira rápida e também porque **falta uma gestão efetiva do que precisa ser remediado**, pois não há um controle centralizado do que deve ser feito.

Falta comunicação entre os times de profissionais na hora de solucionar as vulnerabilidades. Algo que exige das empresas novas técnicas de gestão para notificar e estabelecer prazos para a mitigação dos riscos e vulnerabilidades.

Priorização contextualizada

A priorização contextualizada ajuda líderes de negócios a lidar com as vulnerabilidades mostrando quais sistemas estão expostos e quais estão protegidos e entender quais fazem parte da infraestrutura de processos essenciais e quais desempenham funções menos importantes no negócio. Com isso, as empresas podem transformar a gestão de vulnerabilidades em um método prático baseado em dados e contexto.

A maior dificuldade na adoção dessa abordagem, no entanto, é a falta de integração entre tecnologias de segurança. As ferramentas de escaneamento, por exemplo, não levam em consideração os dados de firewalls, roteadores e outros sistemas de proteção. Por isso, os times de TI acabam com um grande volume de dados de vulnerabilidades e ameaças nas mãos, porém, não conseguem visualizá-los da maneira apropriada para priorizá-los adequadamente com base no contexto do negócio.

Detecção contínua

O processo de obtenção de informações de vulnerabilidades e ameaças é crítico no processo de gestão de vulnerabilidades. As empresas brasileiras carecem de um processo contínuo para coleta, análise e classificação de vulnerabilidades. A periodicidade média das análises de segurança das empresas pesquisas é trimestral com foco em infraestrutura e anual para aplicações.

Isso demonstra baixa maturidade e acarreta em situações de extremo risco para o negócio.

Janelas de correção

Além de não conseguir priorizar corretamente, as empresas brasileiras, muitas vezes, não contam com a agilidade e as informações necessárias para solucionar as vulnerabilidades. Em todos os setores, é grande a quantidade de softwares desatualizados e sem pacotes de segurança críticos, por exemplo.

Com a ascensão dos ataques com alvo e das vulnerabilidades do tipo zero-day, é cada vez mais importante que as empresas diminuam o tempo entre a descoberta de uma vulnerabilidade e sua remediação.

Engajamento de todos os envolvidos no processo

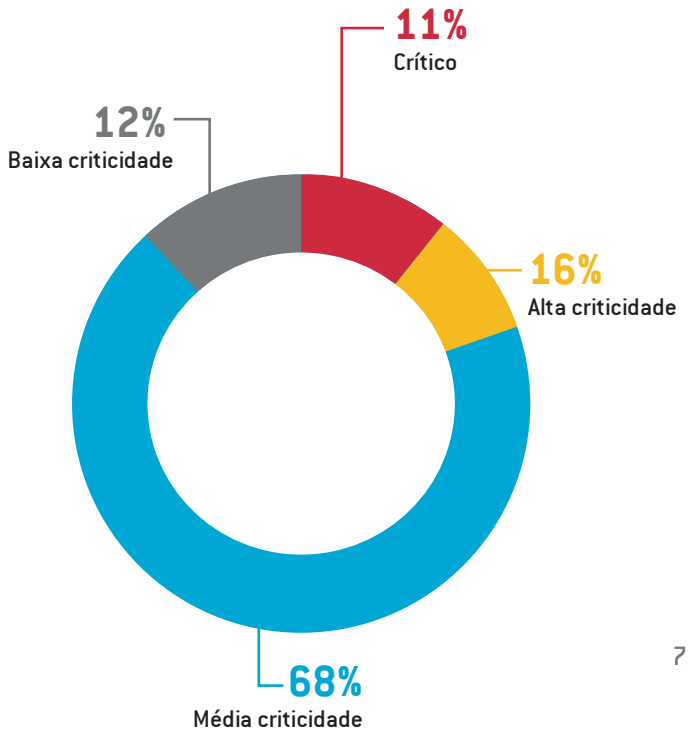
O fator humano tem um grande peso na efetividade dos processos de gestão de vulnerabilidades. Como os sistemas não são integrados, o trabalho acaba mais difícil quando existem múltiplas equipes de TI cuidando da segurança de diferentes áreas do ambiente.

Mesmo que a empresa conte com as melhores ferramentas de segurança, é impossível priorizar riscos de maneira apropriada sem que haja uma boa comunicação entre profissionais atuando em diferentes equipes e departamentos.

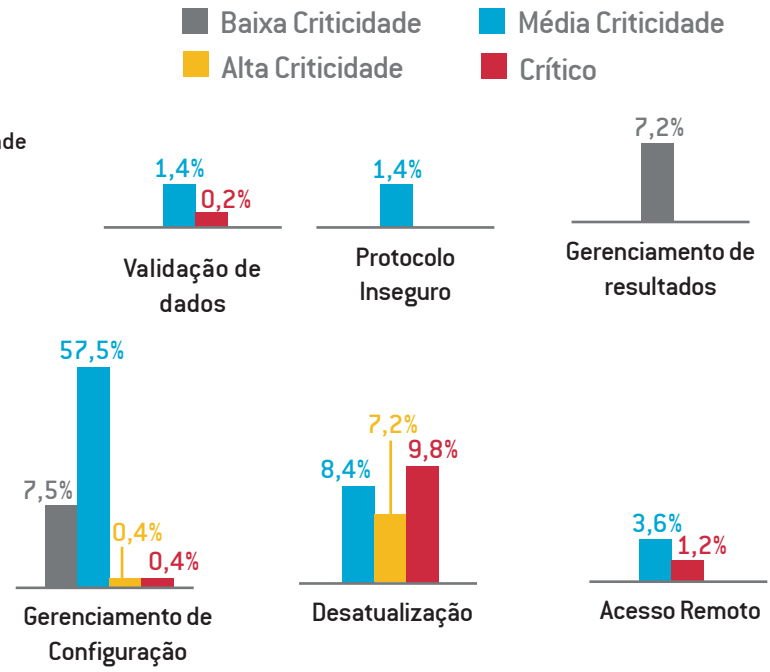
Resultados detalhados de cada setor

CARTÕES

Cartões - Nível de criticidade



Vulnerabilidades no setor de cartões



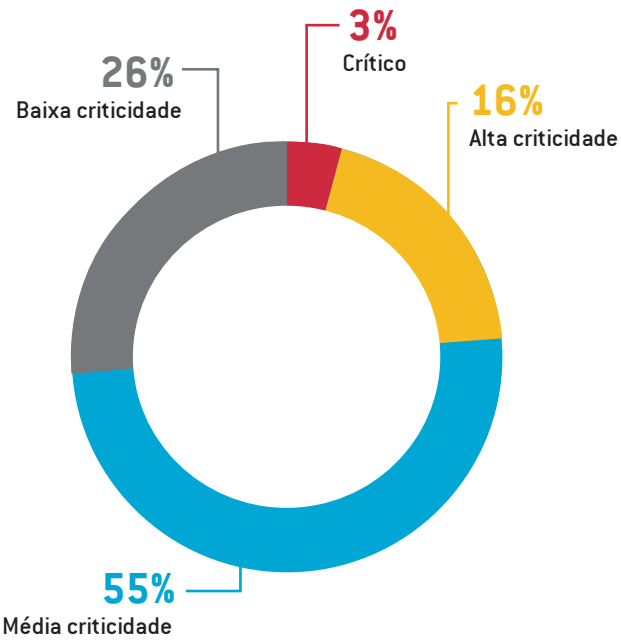
No setor de cartões, as falhas de gerenciamento de configuração de média criticidade são, de longe, as mais comuns. Dentro dessa categoria, destacam-se, principalmente, as falhas que fazem com que o sistema operacional permita a realização de conexões anônimas (Null Session).

As vulnerabilidades que permitem ataques do tipo man-in-the-middle, que permitem que os hackers tenham acesso aos dados trafegados, inclusive informações confidenciais, também são comuns no setor.

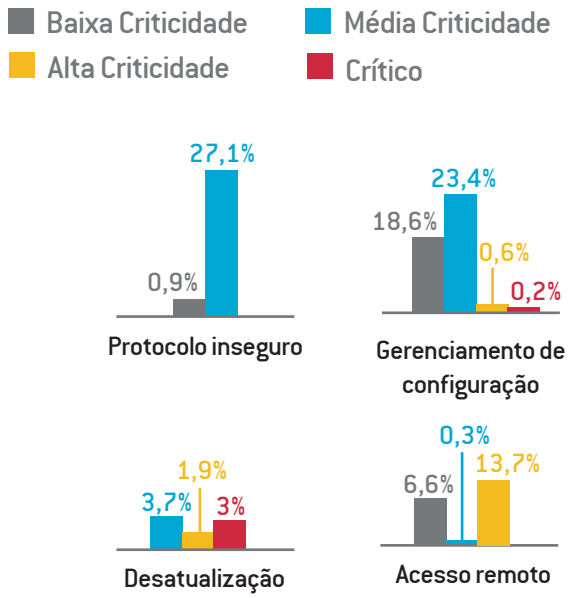
Vulnerabilidade mais comum no setor de cartões:
O sistema operacional permite a realização de conexões anônimas
Falha de segurança de média criticidade

E-COMMERCE

E-Commerce - Nível de criticidade



Vulnerabilidades no setor de e-commerce



No setor de e-commerce apenas **3% das vulnerabilidades foram consideradas críticas**. Destacam-se nos resultados a quantidade expressiva de falhas de segurança relacionadas a protocolos inseguros. Nesta categoria, o setor de e-commerce se sobressai pela quantidade de erros que envolvem chaves criptográficas inadequadas para o protocolo SSL/TLS, algo que pode ser usado por hackers persistentes para quebrar a criptografia de comunicações sigilosas.

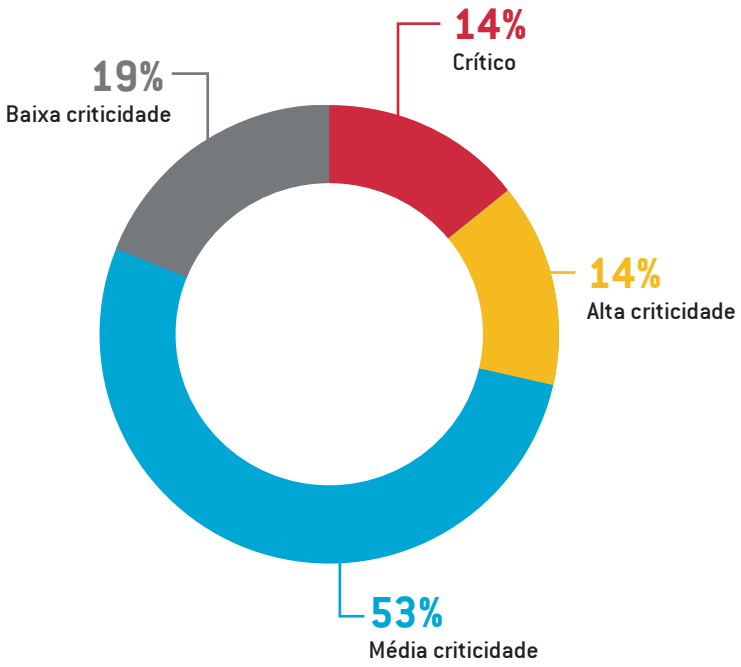
O setor também se destaca pela quantidade de vulnerabilidades de alta criticidade envolvendo acesso remoto. A maioria está relacionada à disponibilidade de acesso ao servidor remotamente, algo que dá aos hackers a possibilidade de invadir o ambiente corporativo e provocar grandes perdas sem muito esforço.

Analisando as vulnerabilidades críticas do setor, vemos que a maioria está na categoria desatualização. Segundo dados da pesquisa, grande parte das falhas de segurança críticas no setor de e-commerce estão relacionadas à falta de pacotes de atualização críticos para componentes como PHP e VMware.

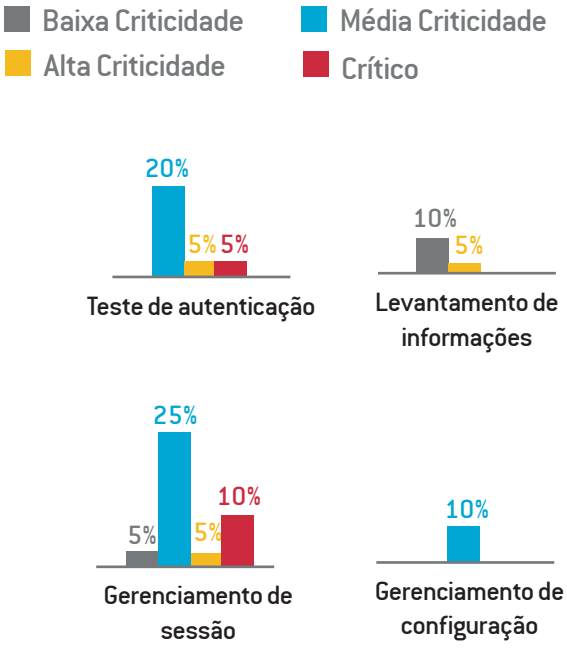
Vulnerabilidade mais comum no setor de e-commerce:
Uso de chaves criptográficas inadequadas para o protocolo SSL/TLS
Falha de segurança de média criticidade

ESPORTES

Esportes - Nível de criticidade



Vulnerabilidades no setor de esportes



No setor de esportes, a maioria das falhas de segurança foram classificadas como de média criticidade, com destaque para as vulnerabilidades de gerenciamento de sessão.

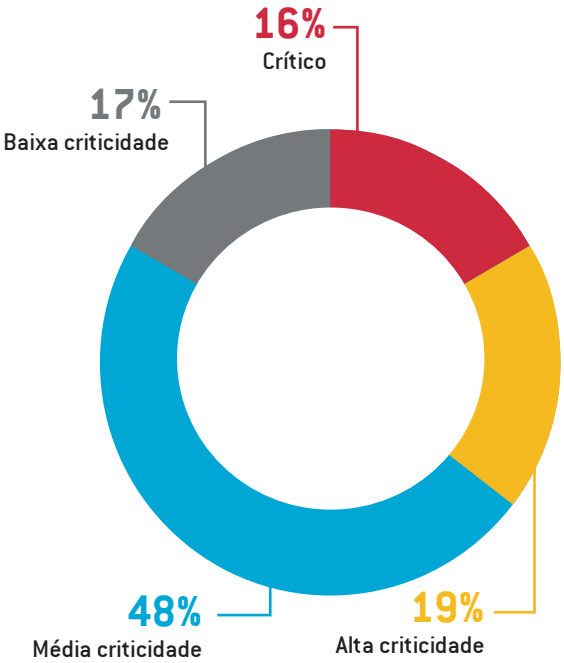
Nessa categoria entram vulnerabilidades de aplicação relacionadas a cookies, como a ausência de atributos como o HTTP Only e o Secure, que garantem mais segurança para o usuário.

Entre as vulnerabilidades críticas encontradas no setor, aparecem a ausência de TLS, o gerenciamento de sessão inadequado e o roubo de sessão.

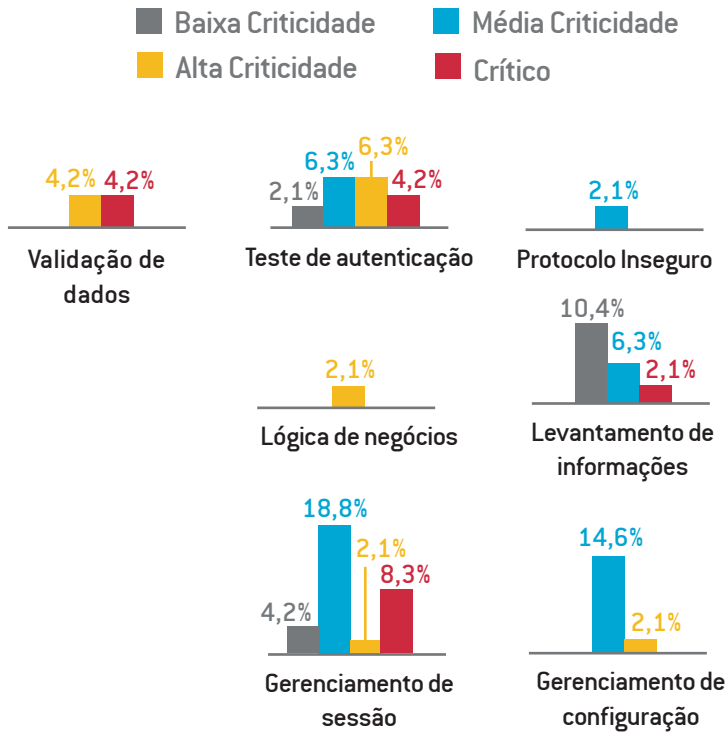
Vulnerabilidade mais comum no setor de esportes:
Cookies com ausência de atributos de segurança
Falha de segurança de média criticidade

FINANCEIRO

Financeiro - Nível de criticidade



Vulnerabilidades no setor financeiro



O Relatório de Ameaças 2016 registra **83% das vulnerabilidades do setor financeiro como falhas críticas e de alta e média criticidade.** O setor é o que conta com a maior porcentagem de vulnerabilidades críticas.

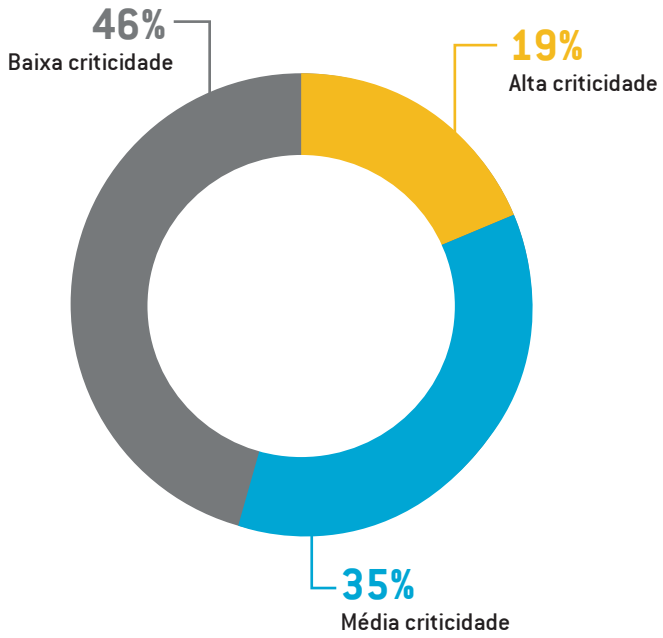
As vulnerabilidades críticas se concentram nas categorias de gerenciamento de sessão, teste de autenticação e validação de dados, todas dizem respeito a falhas de segurança em aplicações.

Entre as brechas críticas, destacam-se as práticas de roubo de sessão, injeção de SQL e gerenciamento de sessão inadequado. Todas essas falhas de segurança podem levar ao comprometimento de toda a infraestrutura de TI e a grandes perdas para o negócio, incluindo paralisações e roubo de dados de clientes.

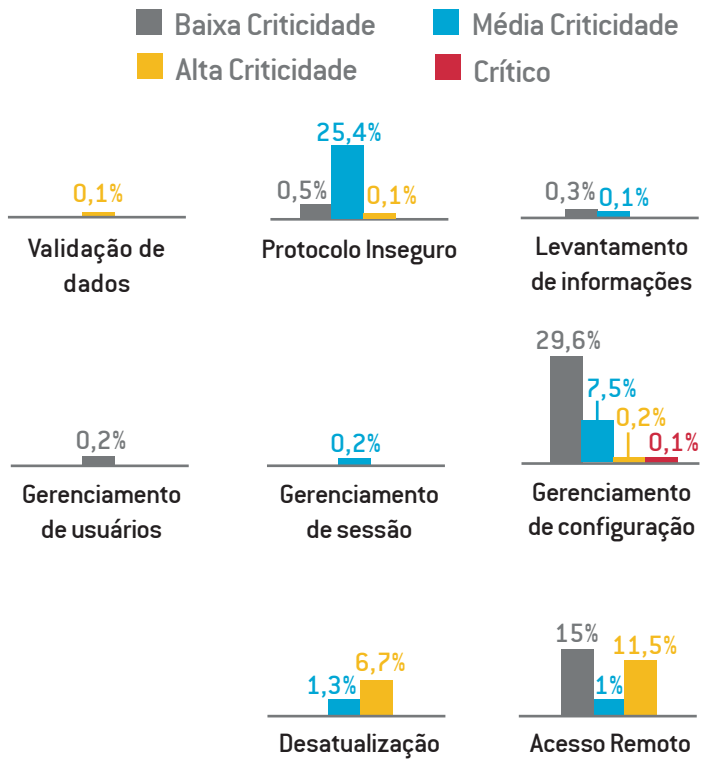
Vulnerabilidade mais comum no setor de e-commerce:
Cookies com ausência de atributos de segurança
Falha de segurança de média criticidade

INDÚSTRIA

Indústria - Nível de criticidade



Vulnerabilidades no setor industrial



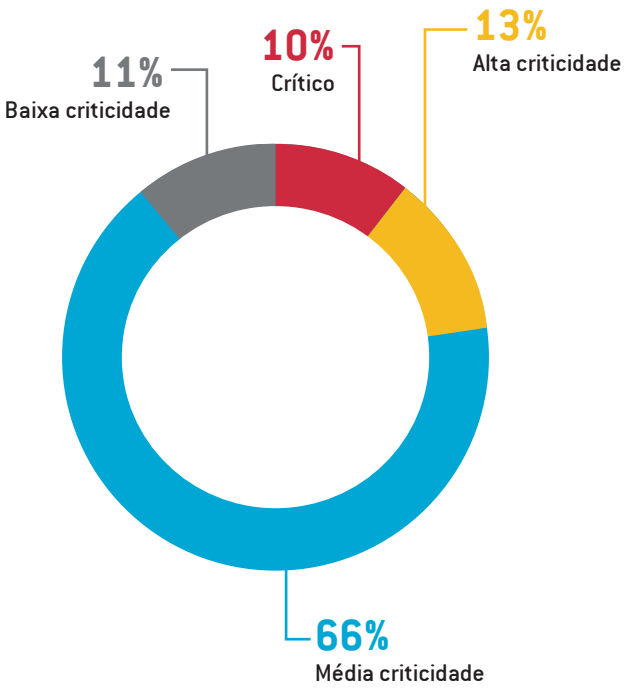
No setor industrial, a quantidade de vulnerabilidades críticas é praticamente nula. A maior parte das vulnerabilidades é de mais difícil exploração (baixa e média criticidade), com destaque para as falhas de gerenciamento de configurações de baixa criticidade, nas quais se sobressai a presença de informações sensíveis disponibilizadas pelo servidor web e a utilização de chaves criptográficas inadequadas pelo serviço de acesso remoto.

As vulnerabilidades relacionadas a protocolos inseguros também são expressivas no setor industrial, especialmente as de média criticidade, nas quais se destaca o uso de chaves criptográficas inadequadas para o protocolo SSL/TLS, erro que pode expor comunicações sigilosas aos cibercriminosos. Também é comum a presença de certificados SSL assinados por autoridades certificadoras desconhecidas.

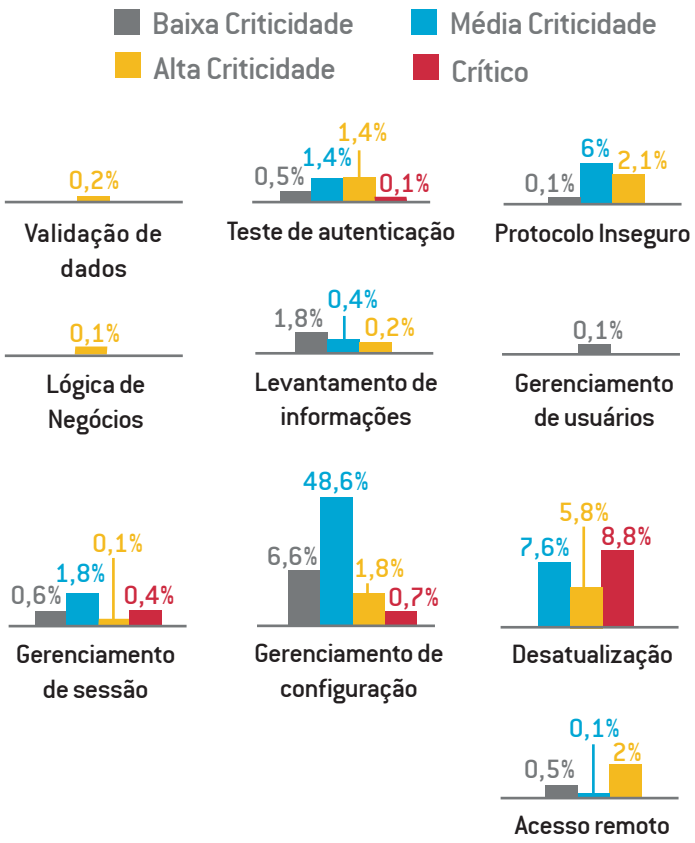
Vulnerabilidade mais comum no setor industrial:
Uso de chaves criptográficas inadequadas para o protocolo SSL/TLS
Falha de segurança de média criticidade

INTERNET

Internet - Nível de criticidade



Vulnerabilidades no setor de internet



O setor de internet é o que conta com a **maior porcentagem de vulnerabilidades críticas e de alta e média criticidade, chegando a 89%**. Apenas **11% vulnerabilidades encontradas no setor foram classificadas como de baixa criticidade**.

Assim como vários outros setores analisados pelo relatório, as falhas de gerenciamento de configurações de média criticidade são as mais comuns. Dentre elas, destacam-se as falhas que deixam o OpenSSL vulnerável a vazamentos de informações sensíveis (POODLE), permitindo a incidência de ataques do tipo man-in-the-middle, no qual os hackers têm acesso a dados trafegados.

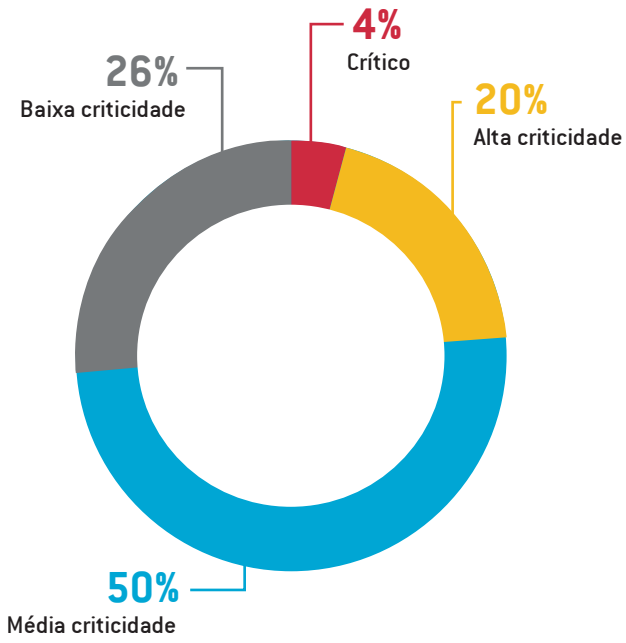
Entre as vulnerabilidades críticas, o destaque fica com as falhas de atualização. A presença de sistemas desatualizados é constante entre as empresas do setor de internet, com a ausência de pacotes de atualização críticos para sistemas como o Windows, PHP e Apache.

Sistemas desatualizados são grandes oportunidades para os hackers, que se aproveitam de vulnerabilidades conhecidas e não solucionadas para invadir a rede e executar diversos tipos de ataque, causando danos aos dados e grandes paralisações, gerando perdas de receita e prejudicando a reputação.

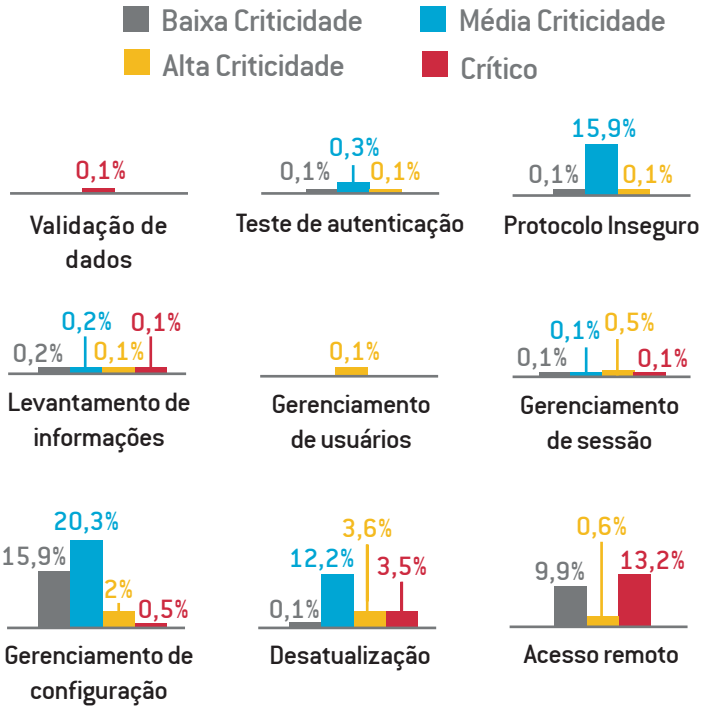
Vulnerabilidade mais comum no setor de internet:
O OpenSSL está vulnerável a vazamento de informações sensíveis (POODLE)
Falha de segurança de média criticidade

LOGÍSTICA

Logística - Nível de criticidade



Vulnerabilidades no setor de logística



No setor de logística se destacam as falhas de média criticidade categorizadas como falhas de gerenciamento de configurações e protocolo inseguro, e as falhas de alta criticidade relacionadas ao acesso remoto.

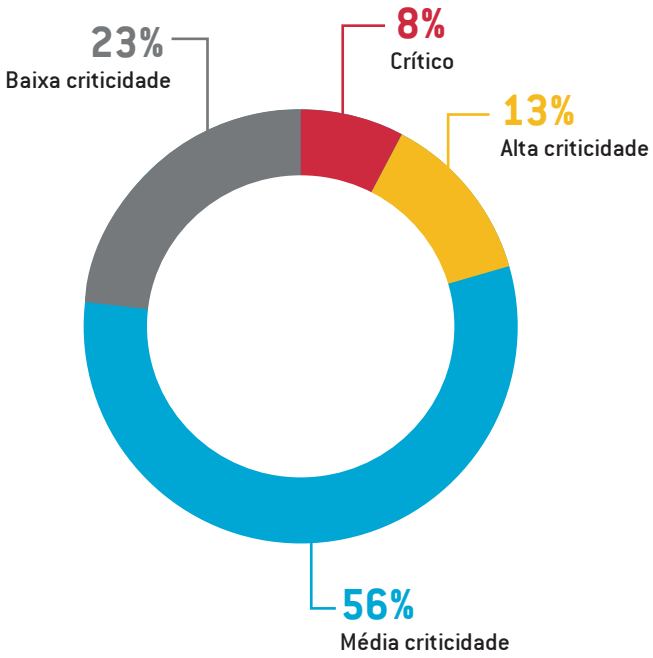
4% das vulnerabilidades do setor foram classificadas como críticas. A maioria está relacionada a falhas de atualização, incluindo não apenas a ausência de pacotes de atualização críticos para diversos softwares, mas a possibilidade de execução de código remoto, que pode comprometer totalmente o funcionamento dos sistemas essenciais.

Entre as falhas de gerenciamento de configurações mais comuns está a possibilidade de realizar de conexões anônimas.

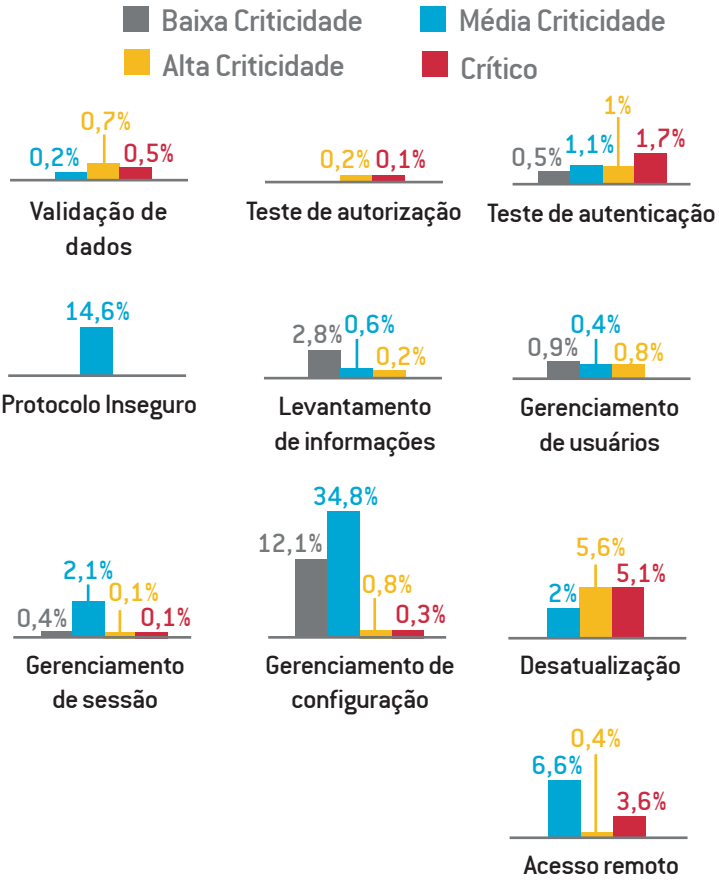
Vulnerabilidade mais comum no setor de logística:
O sistema operacional permite a realização de conexões anônimas
Falha de segurança de média criticidade

SEGUROS

Seguros - Nível de criticidade



Vulnerabilidades no setor de seguros



No setor de seguros, destacam-se as vulnerabilidades de média criticidade relacionadas a falhas de gerenciamento de configurações e protocolos inseguros.

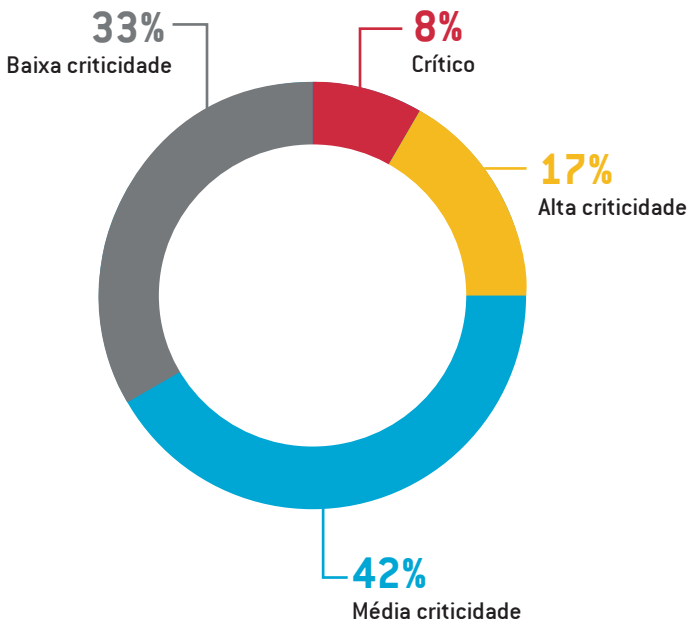
Entre as vulnerabilidades mais comuns estão as falhas que permitem ataques do tipo *man-in-the-middle*, especialmente erros que deixam o OpenSSL vulnerável ao vazamento de informações sensíveis. Em relação aos protocolos inseguros, um dos erros mais encontrados é a utilização de chaves criptográficas inadequadas para o protocolo SSL/TLS.

Entre as vulnerabilidades críticas, a mais comum é relacionada ao Microsoft Schannel, um provedor que implementa protocolos como o SSL e TLS. Uma das falhas mais encontradas no setor de seguros é a possibilidade de executar códigos remotos por meio dessa ferramenta, o que pode expor toda a infraestrutura de TI.

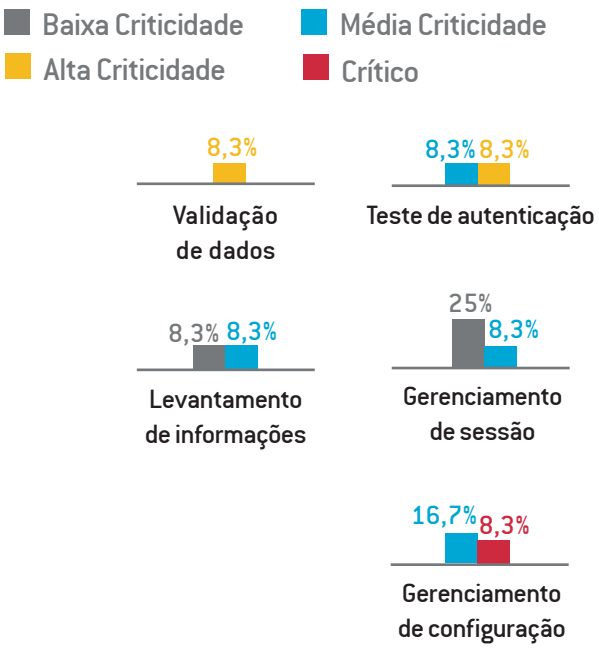
Vulnerabilidade mais comum no setor de seguros:
Componentes vulneráveis a ataques do tipo *man-in-the-middle*
Falha de segurança de média criticidade

TECNOLOGIA

Tecnologia - Nível de criticidade



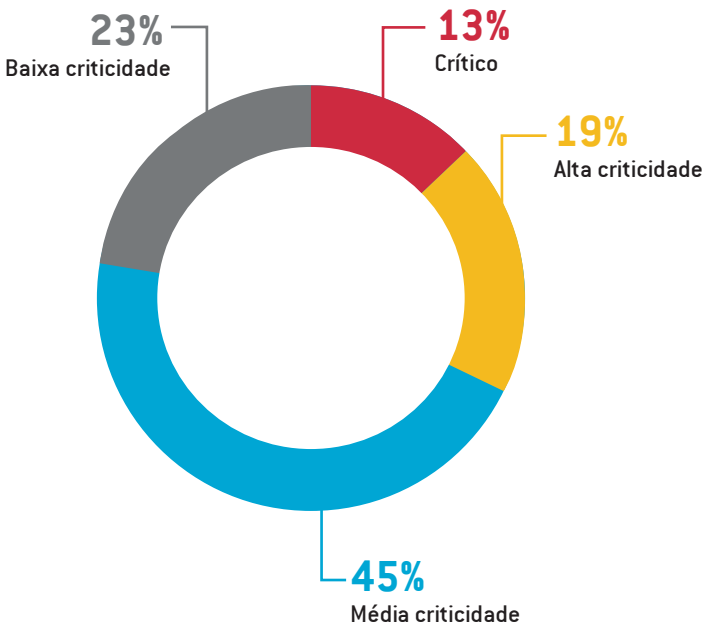
Vulnerabilidades no setor de tecnologia



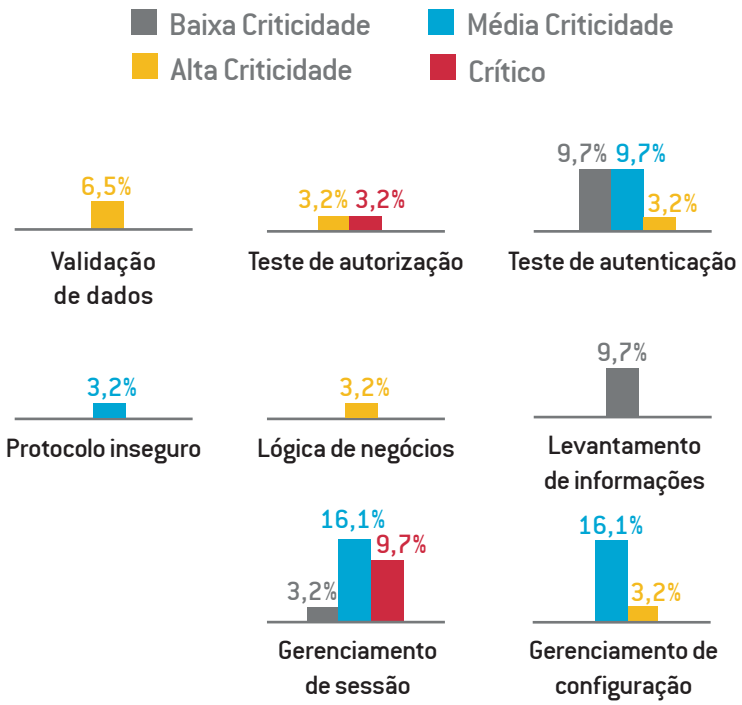
No setor de tecnologia, destacaram-se poucas vulnerabilidades críticas, entre elas está uma falha de gerenciamento de configuração que permite a exposição do código fonte e pode ser extremamente prejudicial para o negócio, pois pode revelar dados como endereço, usuário e senha de bancos de dados, além de lógicas confidenciais.

TELECOMUNICAÇÕES

Telecomunicações - Nível de criticidade



Vulnerabilidades no setor de telecomunicações



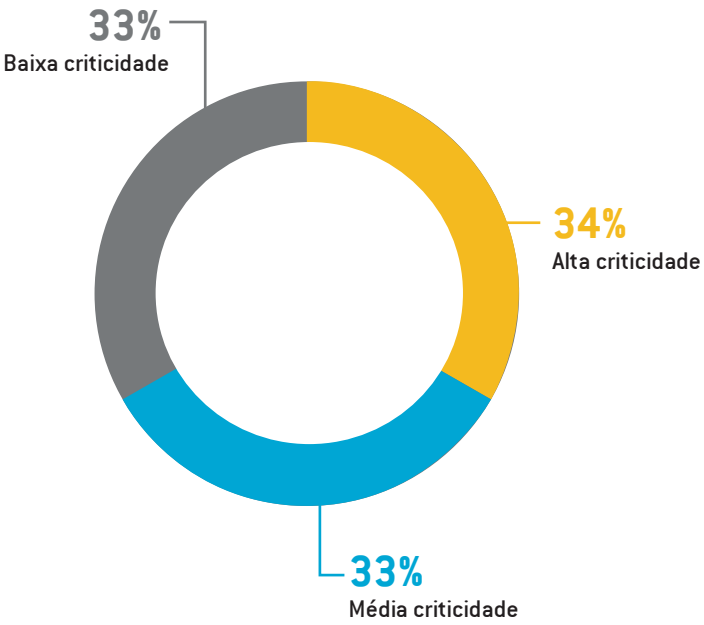
Nos últimos 12 meses, **13% das vulnerabilidades no setor de telecomunicações foram consideradas críticas**. A maioria das falhas de segurança críticas foram classificadas como falhas de gerenciamento de sessão, incluindo o gerenciamento inadequado e o roubo de sessão.

As falhas de média criticidade envolvendo gerenciamento de sessão e gerenciamento de configurações são as mais comuns no setor de telecomunicações, principalmente a ausência de atributos de segurança em cookies.

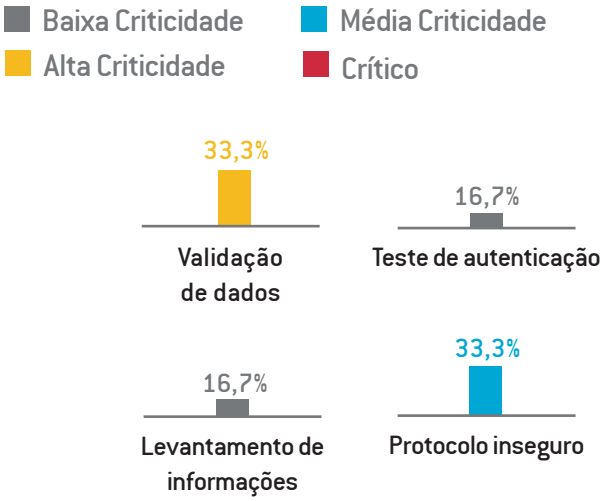
Vulnerabilidade mais comum no setor de telecomunicações:
Cookies com ausência de atributos de segurança
Falha de segurança de média criticidade

VAREJO

Varejo - Nível de criticidade



Vulnerabilidades no setor de varejo



Nenhuma vulnerabilidade foi classificada como crítica no setor de varejo. Houve a mesma quantidade de falhas de segurança de alta, média e baixa criticidade, com destaque para as falhas de gerenciamento de sessão e validação de dados.

Entre as vulnerabilidades mais comuns estão a ausência de atributos de segurança a cookies, com criticidade de nível médio, e o redirecionamento de URL, algo considerado altamente crítico.

O redirecionamento de URL pode ser usado por hackers para redirecionar clientes legítimos para um endereço arbitrário. Essa prática pode ser usada, por exemplo, em campanhas de phishing e outros ataques de engenharia social e pode ser altamente prejudicial para o varejo, que corre o risco de perder vendas e a confiança do cliente.

Vulnerabilidade mais comum no setor de varejo:
Redirecionamento de URL
Falha de segurança de alta criticidade

PARTE 3: COMO MELHORAR OS INDICADORES

A iBLISS, empresa especializada em segurança digital, é referência nacional em desenvolvimento e fornecimento de soluções estratégicas para a proteção de negócios e pessoas, oferecendo programas específicos para diferentes setores da indústria para apoiar todas as atividades que requerem um alto grau de expertise.

Confira alguns dos nossos serviços e soluções que podem ajudar sua equipe de TI a melhorar a gestão de vulnerabilidades e criar um plano consistente de remediação:

Testes de invasão

Os testes de invasão, também conhecidos como pen-tests, permitem às empresas verificar a eficácia de sua estratégia de segurança, bem como as tecnologias adotadas para proteger o ambiente, a rede, os servidores, as aplicações, os serviços e qualquer outra interface.

Entre os benefícios está a possibilidade de determinar o nível de exposição do ambiente e identificar a possibilidade de vazamentos e fraudes. A equipe de segurança da iBLISS conta com um alto nível de expertise, que garante a eficácia de testes manuais que simulam fielmente o modo de ação de cibercriminosos que possam atacar a rede.

Testes Gerenciados

Por meio dos Testes de Segurança Gerenciados, a iBLISS oferece às empresas a possibilidade de solicitar testes de invasão sob demanda, com um tempo de atendimento personalizado e execução de testes customizada de acordo com a necessidade.

Entre os benefícios dos testes de segurança gerenciados está a otimização do tempo da equipe de TI, que pode se concentrar em questões mais importantes, como a definição da estratégia de segurança, e a maior agilidade por meio de um contrato único.

MonSEC

Por meio do MonSEC, a iBLISS oferece um serviço de monitoramento contínuo usando o conceito de Unified Security Monitoring (USM), que permite a integração de soluções de segurança em uma única plataforma. Com isso, os profissionais de TI conseguem gerar um fluxo constante de Inteligência em segurança, tornando possível uma abordagem mais proativa.

O iBLISS MonSEC facilita a identificação de ameaças e incidentes e seu processo de remediação, emitindo alertas automáticos de comportamentos anômalos.

Teste de aplicação Full-Stack

Por meio de uma metodologia exclusiva, a iBLISS verifica toda a extensão da aplicação web por mais de 70 tipos de ataques e vulnerabilidades para identificar pontos de atenção.

Com isso, as empresas podem encontrar vulnerabilidades e falhas em uma aplicação existente, com a perspectiva de auditoria. As organizações têm acesso a um relatório técnico contendo detalhes das vulnerabilidades, forma de reprodução e referências para correção.

GAT

O GAT é uma solução exclusiva da iBLISS que oferece gestão de vulnerabilidades de forma integrada, dando uma visão total do grau de exposição do ambiente de TI, incluindo servidores, rede, aplicações, processos e auditorias.

Com o GAT, as equipes de segurança podem priorizar o tratamento de ameaças com base em informações de diversas plataformas de TI, facilitando a melhoria contínua da segurança e mantendo a conformidade com políticas internas e regulamentações.

iBLISS

FALE CONOSCO

Entre em contato para conhecer nossas soluções

Fone: (11) 3255-3926
Email: contato@ibliss.com.br

Acesse nosso site:
www.ibliss.com.br