# A IMPORTÂNCIA DA GESTÃO DE PATCHES E ATUALIZAÇÕES DE SOFTWARES NO AMBIENTE CORPORATIVO[1]

Jean Carlos Bormanieri

**Resumo**: Vivemos em um mundo onde a informação é o ativo mais valioso que as empresas e pessoas podem ter. Dessa maneira, podemos afirmar que o roubo de informações passou a ser uma ação frequente dos criminosos, que utilizam diversas táticas e técnicas para esse fim. Entre elas, uma das mais utilizadas é a exploração de vulnerabilidades de softwares. Os softwares são produtos inacabados e necessitam de constante desenvolvimento por parte de seus desenvolvedores, seja para evolução tecnológica da solução ou correção de problemas encontrados. Os usuários mal-intencionados exploram esses problemas encontrados nos programas para conseguir acessos não-autorizados e consequentemente comprometer as informações remotas. Este trabalho realizou uma pesquisa buscando avaliar como pequenas e médias empresas estão tratando desse cenário e avaliar se elas estão vulneráveis a ataques que abordam esse tipo de técnica.

**Palavras-chave**: Gerenciamento de Patches. Vulnerabilidades de Softwares. Sistemas Operacionais.

## 1 INTRODUÇÃO

Nos últimos anos, observamos um crescente número de relatos de ataques que exploram vulnerabilidades de aplicativos e sistemas operacionais. Grande parte dessas vulnerabilidades exploradas nesses ataques já possuem correções disponibilizadas pelos seus responsáveis e poderiam ser evitadas caso estivessem aplicadas corretamente nos ambientes das empresas.

Segundo Lento (2011), a informação é o maior patrimônio que uma organização pode possuir se deseja manter-se competitivo. Vivemos em um cenário globalizado onde as organizações possuem diversas necessidades operacionais, e demandam da utilização dos mais diversos tipos de aplicativos para cumprir essas necessidades.

---

[1] Artigo apresentado como Trabalho de Conclusão do Curso de Especialização em Gestão de Segurança da Informação, da Universidade do Sul de Santa Catarina, como requisito parcial para a obtenção do título de Especialista em Gestão de Segurança de TI.

Conforme E-Security Planet (2017), uma rede corporativa é composta de diversos servidores e estações de trabalho, que executam um grande número de diferentes aplicações. Muitas dessas aplicações são disponibilizadas por terceiros e mesmo as empresas que desenvolvem suas próprias soluções por muitas vezes acabam utilizando plugins externos embarcados em suas soluções internas. Até mesmo soluções que possuem demandas legais, como por exemplo, aplicativos relacionados ao governo federal, possuem seu desenvolvimento baseado em plugins como o Java. Conforme o informe de segurança Veracode (2016), 97% de todas as aplicações Java avaliadas pela equipe de segurança deles no ano de 2016 tinham pelo menos um componente com uma vulnerabilidade conhecida.

Visando minimizar riscos e falhas de vulnerabilidades, os desenvolvedores responsáveis pelos sistemas disponibilizam periodicamente atualizações, essas conhecidas como patches. Thetechangel (2017) afirma que existem 3 razões principais para manter os softwares atualizados:

a) Resolver os problemas efetivos existentes no software: Os softwares podem conter problemas lógicos em seu desenvolvimento que podem levar a resultados inesperados ou incorretos. As equipes responsáveis pelo desenvolvimento do aplicativo podem fornecer correções pontuais baseados no feedback dos usuários ou mesmo na evolução do sistema;
b) Resolver problemas de segurança, que podem comprometer a confidencialidade, integridade ou disponibilidade das informações: Dependendo do problema de segurança existente, esse conjunto de propriedades que caracterizam a segurança da informação (LANDWEHR,2001; BISHOP,2003) podem ser comprometidas;
c) Softwares que demandam atualizações regulares para manter a eficácia de seu funcionamento: Como exemplo desses casos, podemos citar os aplicativos de segurança (Exemplo: Antivírus). Segundo Wrightoncomputers (2017), novos vírus e tipos de ameaças surgem todos os dias, o que pode representar uma grande ameaça aos computadores que não conhecem essas novas ameaças;

Considerando essas informações, é dever de todo administrador de sistema compor uma solução que vise criar mecanismos para identificar, validar e atualizar as demandas de softwares dentro de sua organização. Dessa forma, o presente artigo teve como objetivo avaliar como pequenas e médias empresas atuam nesse processo e identificar a importância que uma implantação de um processo de gerenciamento de patches traz para o ambiente. Foi desenvolvido um questionário com perguntas focadas para administradores de rede de empresas de pequeno e médio porte, que abordam processos de gerenciamento de atualizações de sistemas operacionais e aplicativos, além de procedimentos voltados a zelar pela qualidade da gestão de segurança da TI.

## 2 GESTÃO DE PATCHES E ATUALIZAÇÕES NAS PEQUENAS E MÉDIAS EMPRESAS

As empresas possuem grande dificuldades em manter o seu parque de computadores com softwares atualizados. Conforme Computerworld (2017), manter os sistemas desatualizados é a vulnerabilidade crítica mais comum no Brasil. Eles apontam que 92% das vulnerabilidades críticas de infraestrutura correspondem a falhas de atualização.

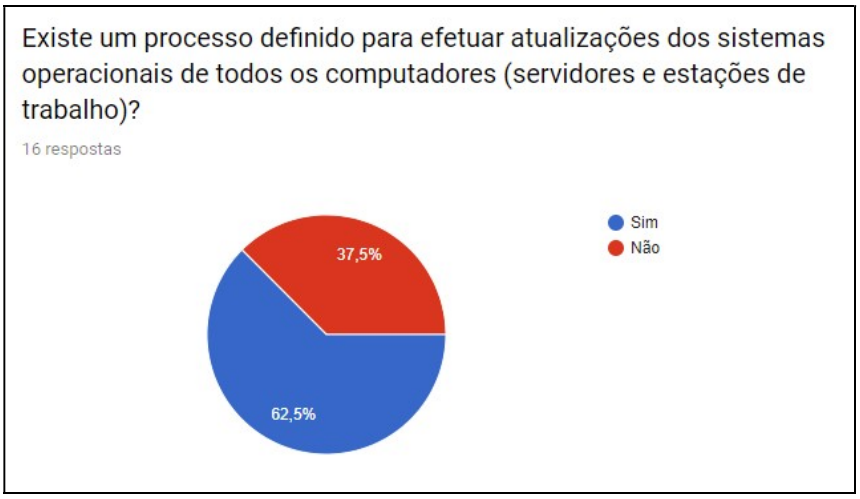
No Brasil, cerca de 99% das empresas são compostas por empresas de micro e pequeno porte (PROFISSIONAISTI,2014). Nessas empresas a área de TI é normalmente tratada como uma área secundária e não estratégica para a empresa, e logo, não recebe os investimentos necessários para garantir a segurança da informação. Baseado nessa concepção, essa pesquisa foi focada em avaliar os cenários da gestão de gerenciamento de patches e atualizações de softwares de pequenas e médias empresas.

### 2.1 ANÁLISE DE DADOS - GESTÃO DE PATCHES DE SISTEMAS OPERACIONAIS

Conforme resultado da pesquisa realizada e descrito no Gráfico 1, cerca de 37,5% das empresas não possui nenhum processo focado na gestão de atualizações dos sistemas operacionais. Além disso, das empresas que informam que possuem processo definido (62,5% das empresas avaliadas), quase todas informam que fazem uso apenas do WSUS (Windows Software Updates Services), ferramenta essa que abrange exclusivamente atualizações de produtos Microsoft. Segundo Exame (2014), 78% das empresas brasileiras possuem o sistema

operacional Windows (desenvolvido e mantido pela Microsoft) em seu parque de computadores e 41% delas também possuem sistemas operacionais Linux operando em seu parque.

Gráfico 1- Processo de Gestão para Atualizações de Sistemas Operacionais




Fonte: Elaborado pelo Autor (2017).

Apesar de observarmos que a imensa maioria das empresas adotam como padrão sistemas operacionais da Microsoft, vemos através da pesquisa que outras plataformas (mesmo que existentes no ambiente) ainda são completamente ignoradas no que tange a processos de atualizações. Essas plataformas abertas possuem desenvolvimento contínuo pela comunidade e dessa maneira recebem constantes atualizações, tanto relacionadas a evolução do software como correção de vulnerabilidades. As pequenas e médias empresas avaliadas ficam expostas a ataques externos devido a essa falta de um processo definido para gestão na atualização dessas plataformas.

Empresas que não realizam nenhum tipo de gestão no processo de atualizações de sistemas operacionais são alvos fáceis de usuários mal-intencionados. Existem várias vulnerabilidades conhecidas e consideradas críticas, pois expõem o computador a ataques remotos sem a necessidade de execução de um gatilho, ou seja, quando bem exploradas elas permitem que o atacante realize o ataque nem a necessidade de nenhuma intervenção ou execução de programas locais.

## 2.2 ANÁLISE DE DADOS - GESTÃO DE PATCHES DE SOFTWARES DE TERCEIROS

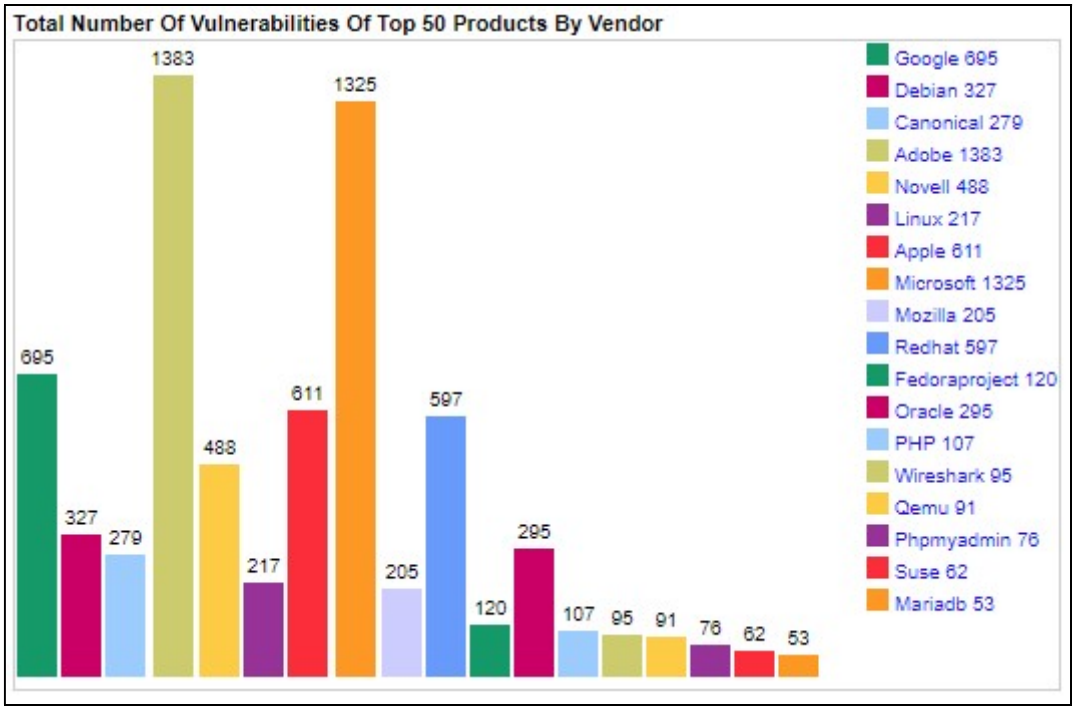
Segundo o questionário desenvolvido e dados visualizados no Gráfico 2, 75% das empresas não possui nenhum tipo de processo voltado a atualizações de aplicativos de terceiros. Cve Details (2017) descreve que no ano de 2016, a Adobe foi a empresa com o maior número de vulnerabilidades no mundo, ou seja, em uma realidade onde a maioria das empresas implementam processos que focam somente na atualização de produtos Microsoft, essas empresas ficam completamente vulneráveis quando utilizam softwares de outras empresas.

Gráfico 2 - Processo de Gestão para Atualizações de Programas de Terceiros nas Empresas Avaliadas


Fonte: Elaborado pelo Autor (2017).

Como podemos observar na Figura 1, no último ano foram descobertas e documentadas milhares de vulnerabilidades nos mais diversos tipos de softwares. Muitas dessas vulnerabilidades possuem classificação crítica e podem fornecer acesso remoto a usuários mal-intencionados quando exploradas com sucesso.

Figura 1 – Total de Vulnerabilidades dos Maiores 50 Produtos por Empresa 2016




Fonte: CVE DETAILS (2016).

O impacto preciso que uma vulnerabilidade abrange e que se pode ser corrigido com um patch é difícil de determinar, conforme Welivesecurity (2016). A extensão da gravidade ou a abrangência do problema exige uma análise técnica profunda e individual, cenário que nas empresas nem sempre existe. A grande quantidade de softwares existentes nas organizações dificulta muito esse trabalho, sendo que os responsáveis técnicos nem sempre possuem total conhecimento de seu parque computacional. Dessa maneira, ao não adotar processos que visem avaliar e implantar a instalação de patches necessários a esses softwares de terceiros, as empresas ficam expostas e podem ter seus dados comprometidos.

## 2.3 ANÁLISE DE DADOS - TRÁFEGO CRIPTOGRAFADO

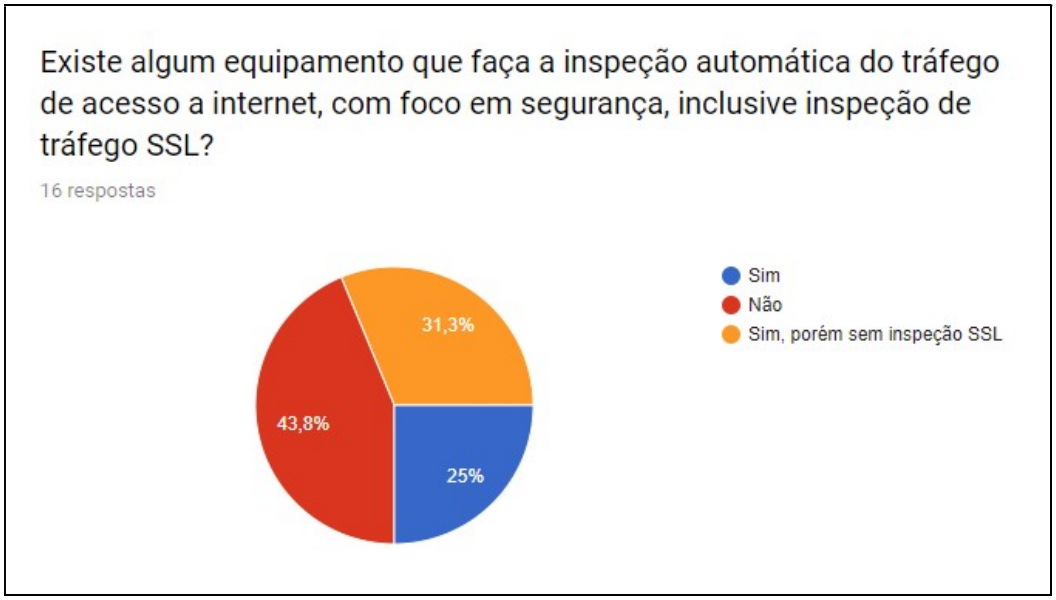
Nos últimos anos, mudanças fundamentais no panorama de desenvolvimento de aplicativos têm corroído a segurança que os firewalls tradicionais forneciam (PALOALTO,2017). As empresas, focando em melhorar a segurança e confidencialidade dos dados trafegados, passaram a desenvolver seus aplicativos incorporando protocolos de criptografia para o tráfego de dados. Esses protocolos normalmente utilizam a porta 443, o

que acaba dificultando a análise dos dados feitos pelos modelos de firewall tradicionais. Somente firewalls com o conceito de Next Generation Firewall conseguem interceptar e avaliar o conteúdo criptografado trafegado, afim de identificar as aplicações e aplicar as regras definidas pela organização.

Conforme Xtechcommerce (2017), o uso do protocolo SSL ou TLS provê a privacidade e a integridade de dados entre duas aplicações que comuniquem pela internet. Isso ocorre por intermédio da autenticação das partes envolvidas e da cifragem dos dados transmitidos entre as duas partes. Resumidamente, podemos afirmar que o uso dessa técnica impede que alguma informação seja interceptada e alterada, garantindo assim mais segurança na troca de informações na internet.

Partindo dessa informação, os usuários mal-intencionados estão utilizando essa técnica criptografando o tráfego de seus programas afim de esconder ameaças avançadas (COMPUTERWORLD,2017). Segundo Eweek (2017), nos primeiros seis meses de 2017 autores e operadores de malwares mais que dobraram o uso dessa técnica, visando buscar anonimato nas comunicações e escapar da detecção de programas de segurança. Como podemos observar na pesquisa realizada e com dados sumarizados no Gráfico 3, essa técnica é altamente eficaz pois cerca de 75% das empresas entrevistadas não possuem equipamentos adequados para avaliar e verificar tráfego criptografado.

Gráfico 3 - Inspeção de Tráfego SSL




Fonte: Elaborado pelo Autor (2017).

Significa afirmar que cerca de 75% das empresas não tem nenhuma gerência no tráfego de dados que utilizam essa técnica, o que possibilita aos usuários mal-intencionados operar e trafegar dados dentro da rede da organização sem serem percebidos.

## 2.4 ANÁLISE DE DADOS - GESTÃO DE ATUALIZAÇÃO DE PROGRAMAS DE SEGURANÇA

Através de nossa pesquisa podemos observar que cerca de 56,3% das empresas não possuem processos de gestão que garantam que seus parques de computadores possuam atualizações eficazes nos softwares de segurança. Vivemos em um momento tecnológico, segundo Computerhowtoguide (2017), onde novas ameaças surgem todos os dias. Devido a isso, por exemplo, a proteção de seu antivírus se torna desatualizada à medida que novas ameaças surgem. Conforme Itforum365 (2016), surgem mais de 300 novas ameaças na internet a cada minuto.

Gráfico 4 - Processo de Gestão de Atualizações de Softwares de Antivírus


Fonte: Elaborado pelo Autor (2017).

Conforme Sans Institute (2017), um dos grandes problemas em manter o software antivírus atualizado é que sempre os desenvolvedores de malwares estão um passo a frente das empresas de segurança, pois o próprio conceito tradicional das ferramentas de antívirus é

a criação de vacinas baseadas em amostras de vírus existentes. Dessa maneira, a ameça após ser criada e divulgada na internet precisa ser identificada, analisada através de engenharia reversa e a empresa de segurança precisa elaborar uma vacina baseada nos resultados. Somente após esse processo ela disponibiliza essa vacina para que seus softwares clientes façam o processo de atualização.

Além do carater operacional, existe o problema da implantação dessas atualizações nos computadores dentro das organizações. Muitos gestores optam pela utilização de versões grátis de soluções de segurança, o que acaba dificultando o trabalho para a equipe de TI pois normalmente essas soluções gratis são autônomas e não possuem versões que possam serem gerenciadas e policiadas remotamente. Dessa maneira, somente é possível garantir que os computadores possuam as vacinas mais atualizadas efetuando a atualização manualmente em cada computador. Diferentemente, as soluções de segurança pagas costumam ter serviços adicionais agregados, como ferramentas de gerenciamento remoto e camadas de proteções específicas adicionais.

## 3 SOLUÇÕES PROPOSTAS

Baseado nos dados evidenciados no questionário e na pesquisa realizada, avaliamos que as pequenas e médias empresas em geral estão vulneráveis a ataques que exploram vulnerabilidades em sistemas operacionais e aplicativos. Elas não implementam processos que mitigam por completo esse cenário, ficando assim expostas a ameaças que podem ser exploradas com sucesso. A seguior enumero algumas ações que poderiam ser adotadas para desenvolver o processo de gestão de patches dentro das organizações orquestradas, e assim diminuir o risco dessas vulnerabilidades:

a) Adoção de ferramentas que contemplem o gerenciamento de todos os sistemas operacionais utilizados no ambiente: Foi observado que algumas empresas implementam ferramentas de atualizações específicas para uma determinada plataforma, ignorando muitas vezes equipamentos que fazem parte de ativos críticos do ambiente. As empresas precisam passar a entender que todos os

ativos existentes no ambiente precisam ser avaliados e atualizados regularmente;

b) Adoção de políticas e regras que busquem aprimorar a implantação desses patches no ambiente: Cada ambiente possui suas características e necessidades próprias, portanto é importante que a equipe responsável pelo gerenciamento do ambiente elabore políticas específicas que atendam às necessidades da organização, implantando uma gestão de patches confiável e funcional, além de diminuir os impactos e transtornos que esse trabalho pode ocasionar;

c) Desenvolvimento de equipe: As empresas devem possuir uma equipe que seja responsável pela implantação do processo de gestão de patches e principalmente por alinhar o cumprimento das regras e políticas definidas. Como o conhecimento do negócio está dentro das organizações, elas são as mais indicadas para avaliarem o impacto que cada tipo de patch ou atualização pode ter no ambiente;

d) Treinamento com foco na segurança da informação: Não somente a equipe de TI, mas todos os colaboradores das organizações deveriam passar por um treinamento voltado para a segurança da informação, afim de conhecer as possíveis ameaças existentes, o impacto que elas podem ocasionar no negócio da empresa e como evitá-las;

## 4 CONCLUSÃO

O mercado competitivo entre as empresas é altamente acirrado. No panorama atual, onde praticamente todos estão conectados e operando na internet, a questão da segurança da informação ainda não é tratada com a devida atenção necessária. Criar políticas e processos para mitigar os riscos e ameaças existentes exige investimentos, desde a capacitação da equipe até mesmo a aquisição de equipamentos e softwares específicos. Dependendo do tamanho da empresa, os valores a serem investidos são altos e o ROI (Return Of Investiment) nem sempre parece claro aos olhos dos gestores. Essa situação é mais contundente em pequenas e médias empresas, que por possuírem um orçamento de investimentos em TI mais limitado acabam direcionando esse montante apenas pra questões

operacionais do dia a dia. Entretanto, diferentemente do que pode parecer, essas empresas podem sofrer consequências tão graves quanto empresas maiores em casos de comprometimento de suas informações por exploração de ameaças de segurança externas, visto que devido a essa restrição orçamentária elas normalmente não estão preparadas para enfrentar esses casos.

Como observado, a vulnerabilidade de softwares é um problema existente e predominante na maioria das pequenas e médias empresas. Devido a não existência de uma padronização na maneira como as empresas desenvolvedoras disponibilizam seus patches, o trabalho de desenvolvimento e implantação de um processo focado na gestão de patches e atualizações de softwares é extremamente complexa. Somado a isso, vemos que a gestão da TI nas empresas é deficitária e atividades simples, porém necessárias, não são realizadas adequadamente. Por exemplo, essas empresas têm grande dificuldade em mapear os ativos de software, fato que contribui para a dificuldade de avaliar e identificar quais os patches devem ser implantados e em quais computadores.

Apesar de existirem ferramentas relacionadas a processos de atualização dos principais fornecedores de sistemas operacionais, e dessas ferramentas normalmente serem disponibilizadas sem custos para as empresas, elas acabam não abrangendo outros tipos de programas existentes dentro das organizações. Para abordar esses casos, a TI das empresas precisa buscar soluções no mercado que façam a gestão dessas atualizações de softwares. Porém essas soluções nem sempre são baratas, além de exigir especialização do time que a gerenciará, esbarrando assim na restrição orçamentária.

Como identificamos na realização dessa pesquisa, as pequenas e médias empresas em geral não implementam processos que garantam o processo de atualização de patches e softwares dentro de suas organizações. Dessa maneira elas ficam expostas a riscos e ameaças externas que utilizam métodos que exploram essas vulnerabilidades. Muitas das ameaças existentes hoje podem facilmente comprometer o funcionamento por completo dessas organizações, visto que elas também não possuem uma gestão adequada da TI com foco na segurança da informação.

# REFERÊNCIAS


BISHOP, M. **Computer security art and sciense.** Addison Wesley, 2003.

COMPUTERHOWTOGUIDE. **Why You Should Update Your Antivirus Software Frequently.** Disponível em: <http://www.computerhowtoguide.com/2012/05/why-update-antivirus-software-frequently.html>. Acesso em: 30 nov. 2017

COMPUTERWORLD. **Desatualização é a vulnerabilidade crítica mais comum no Brasil.** Disponível em: <http://computerworld.com.br/desatualizacao-e-vulnerabilidade-critica-mais-comum-no-brasil>. Acesso em 20 nov. 2017

COMPUTERWORLD**. Hackers usam o tráfego criptografado para esconder ameaças avançadas.** Disponível em: <http://computerworld.com.br/hackers-usam-o-trafego-criptografado-para-esconder-ameacas-avancadas>. Acesso em 23nov. 2017

CVE DETAILS. **Top 50 Products By Total Number Of "Distinct" Vulnerabilities in 2016.** Disponível em: <http://www.cvedetails.com/top-50-products.php?year=2016>. Acesso em 20 nov. 2017

E-SECURITY PLANET. **Patch Management: How to Update Software on Your Network Securely**. Disponível em: <http://www.esecurityplanet.com/network-security/patch-management.html>. Acesso em: 27 ago. 2017

EWEEK**. More Hackers Building SSL Encryption into Malware, Zscaler Finds.** Disponível em: < http://www.eweek.com/security/more-hackers-building-ssl-encryption-into-malware-zscaler-finds>. Acesso em 23nov. 2017

EXAME. **Linux é usado em 41% das empresas brasileiras de TI, aponta pesquisa.** Disponível em: <https://exame.abril.com.br/tecnologia/linux-e-usado-em-41-das-empresas-brasileiras-de-ti-aponta-pesquisa/>. Acesso em 20 nov. 2017

ITFORUM365. **Mais de 300 novas ameaças surgem na internet a cada minuto.** Disponível em: < https://www.itforum365.com.br/seguranca/ameacas/mais-de-300-novas-ameacas-surgem-na-internet-a-cada-minuto/>. Acesso em: 30 nov. 2017

LANDWEHR, Carl E. **Computer security**. Springer-Verlag, 2001.

LENTO, Luiz Otávio Botelho (2011). **Governança e Gestão da Segurança de Informação** Publicado por Universidade do Sul de Santa Catarina

PALOALTO. **Visão geral do firewall de próxima geração.** Disponível em: <https://media.paloaltonetworks.com/documents/datasheet-firewall-feature-overview-pt.pdf>. Acesso em 04 dez. 2017

PROFISSIONAISTI. **A realidade de ambientes de TI em Micro e Pequenas Empresas (MPE).** Disponível em: <https://www.profissionaisti.com.br/2014/02/a-realidade-de-ambientes-de-ti-em-micro-e-pequenas-empresas-mpe/>. Acesso em 20 nov. 2017

SANS INSTITUTE. **Issues with Keeping AntiVirus Software Up to Date.** Disponível em: <https://www.sans.org/reading-room/whitepapers/malicious/issues-keeping-antivirus-software-date-34>. Acesso em: 30 nov. 2017

THETECHANGEL. **Why are updates so important for my computer?** Disponível em: <https://thetechangel.com/knowledge/questions-answers/why-are-updates-so-important-for-my-computer/>. Acesso em: 27 ago. 2017

WELIVESECURITY. **Por que o software é vulnerável? A importância dos patches.** Disponível em: <https://www.welivesecurity.com/br/2016/09/14/importancia-patches/>. Acesso em 02 dez. 2017

WRIGHTONCOMPUTERS. **Why it is important to keep your anti-virus up to date?** Disponível em <http://wrightoncomputers.com.au/important-keep-anti-virus-date/>. Acesso em 27 ago. 2017

XTECHCOMMERCE. **O que é SSL e como funciona.** Disponível em: < https://suporte.xtechcommerce.com/hc/pt-br/articles/204352535-O-que-é-SSL-e-como-funciona->. Acesso em 04 dez. 2017