Aumentando a produtividade e a segurança da sua empresa com o Sophos XG

Marcelo Puntel[1], Felipe Becker Nunes [1], José Luiz Rodrigues Filho[1]

[1]Antonio Meneghetti Faculdade (AMF)

{marcelopuntelc9, nunesfb, joseluiz.rodriguesf} @gmail.com

Abstract. *Currently, the risks of navigating without security is a prime consideration for the personal and professional environment. This article aims to show how the downtime of employees using the internet of their company is high and alert on the dangers of networks and demonstrate why information security it is so important for a company or for themselves. The research was conducted using cases of companies that use the Sophos XG, and graphs were generated from the collected monitoring data. Results demonstrate management in users' access control, and lockouts of apps that can affect business productivity.*

Resumo. *Os riscos de navegar sem segurança é algo primordial a se considerar nos dias atuais, tanto para o meio pessoal e profissional. Este artigo tem como objetivo mostrar como o tempo ocioso dos colaboradores utilizando a internet na empresa é alto e alertar sobre os perigos das redes e demonstrar porque é tão importante para uma empresa ou para si, a segurança da informação. A pesquisa foi realizada utilizando cases de empresas que utilizam a Sophos XG, sendo gerados gráficos foram gerados a partir dos dados de monitoramentos coletados. Os resultados demonstram o gerenciamento no controle de acesso dos usuários, sendo possível realizar bloqueios de aplicativos que podem afetar a produtividade do negócio.*

1. Introdução

No ano de 2017, segundo o Nic.BR (2018), o uso de internet por microempresas chegou a 88%, já em empresas como as de médio e grande porte esse número tende a ser ainda maior. Diante deste contexto, em meio à navegação de centenas de pessoas dentro de uma empresa, a segurança das informações e dados podem ser afetadas por inúmeros fatores, desde o ambiente onde está, pelo próprio usuário e por pessoas que tentam roubar ou modificar as informações. Ferreira et al. (2016) explica que é necessário que as organizações saibam administrar a segurança da informação de forma estratégica, possibilitando que o negócio da organização seja realizado e a sua missão alcançada.

De acordo com Bar (2017), as grandes invasões geralmente se iniciam de pequenas brechas, em que, as vulnerabilidades podem se iniciar até de forma acidental, e o papel da Segurança da Informação é bloquear qualquer possibilidade de risco que uma empresa possa ter. Hoje a má utilização da internet tem afetado e custado muito prejuízo para as empresas, sejam elas de pequeno a grande porte, as piores causas destes problemas vão de o mau uso da internet pelos seus colaboradores no ambiente de trabalho, acessando sites que contém malwares, vírus e ransomwares, que podem infectar a rede deixando-a vulnerável e de fácil acesso.

Para os autores Turban e Volonino (2013), entre os principais erros que os gerentes ou diretores comentem é não dar a devida importância ao assunto, não conhecendo as vulnerabilidades e ameaças presentes na organização. Em consonância com este pensamento, Carvalho (2018) alerta que ameaças e vulnerabilidades se constituem como tema recorrente para entender a segurança da informação, no sentido que se deve conhecer os riscos tecnológicos que existem para as organizações e, assim, tomar as medidas de segurança necessárias.

Diante deste contexto, atualmente existem diversas ferramentas que podem auxiliar na proteção de uma empresa e evitar infiltrações indesejadas em suas redes, como o uso de um antivírus e Firewall. Segundo Kurose (2013), um firewall é uma combinação de hardware e software capaz de isolar uma rede de outras redes, efetuando bloqueios de pacotes que trafegam pela rede com base em políticas e regras previamente definidas.

Turban e Volonino (2013) acreditam que as funções desempenhadas pelos funcionários precisam ser monitoradas permanentemente, como forma de verificar o cumprimento das políticas da organização. Para isso, são necessários equipamentos especializados, que possam conduzir tais ações e fornecer feedbacks em tempo real aos gerenciadores. Uma das empresas que desenvolve esse tipo de equipamento é a Sophos, empresa Inglesa fundada em 1985.

A empresa fornece produtos que incluem a segurança de endpoint de última geração com dispositivos de prevenção avançada contra ameaças, criptografia ativa e Firewall XG. A Sophos conta com uma equipe de pesquisadores de ameaças em sua sede e também rastreia novas variedades de malware. Em 2014, a Sophos adquiriu a empresa Cyberoam Technologies, empresa indiana de produtos de segurança de rede, um deles sendo o XG Firewall, um dos líderes no mercado de segurança e foco do nosso artigo. Portanto, este trabalho tem como finalidade apresentar o uso do software de segurança Sophos XG para averiguar o impacto do uso deste tipo de solução em um ambiente corporativo e indicar indícios de como isto pode afetar na produtividade da empresa, definindo a partir de políticas de acesso, quais conteúdos contidos na internet serão liberados aos colaboradores durante o período de trabalho.

2. Trabalhos Relacionados

Nesta seção, são apresentadas postagens relacionadas ao tema desta pesquisa para que possa haver um conhecimento mais abrangente sobre o assunto citado neste artigo.

O trabalho desenvolvido por Panes (2011) tem como objetivo apresentar um sistema de gerenciamento de regras de firewall, baseado na arquitetura cliente/servidor, que permite manter a coerência das regras aplicadas nos firewalls da empresa. Através da porção servidora do software realiza-se o cadastramento destas regras que garantam a efetividade da aplicação das Políticas de Segurança da empresa, independentemente de onde o cliente esteja localizado. O artigo apresenta dois estudos de casos, um sobre o Sophos Endpoint Security and Data Protection e outro sobre o sistema Symantec Network Access Control 11. Os resultados obtidos demonstram que o software proposto permite gerenciar regras de firewall de forma coerente e adequada.

Na pesquisa conduzida por Carvalho (2018), o objetivo foi averiguar como empresas do ramo financeiro tem gerenciado a segurança da informação em seu âmbito físico e lógico, visto que trabalham com informações sensíveis e valiosas. Um modelo

foi utilizado para realizar a coleta de dados por meio de um survey. Os resultados obtidos demonstraram que o fator humano foi considerado o ponto crítico da segurança da informação na empresa, além de falhas de administração das políticas de segurança.

Os artigos mencionados apresentam uma visão clara da importância em se utilizar ferramentas e políticas de segurança que permitam um gerenciamento mais sólido e constante nas empresas em relação aos acessos à informação. Este trabalho está centrado no mesmo objetivo, tendo como diferencial a amostragem de resultados utilizando a ferramenta Sophos XG que apresentam como os usuários conduzem seus acessos às informações e o perigo envolvente neste contexto.

3. Arquitetura do Experimento

A ferramenta utilizada neste experimento foi o XG firewall (Next Generation) da Sophos, que é um termo de segurança de informações que se refere a uma única solução de segurança, e normalmente é um único dispositivo de segurança que oferece várias funções de segurança em um único ponto na rede (SOPHOS, 2017).

O XG Firewall possui um gerenciamento completo da sua rede e segurança da mesma, de um modo bem dinâmico e de fácil entendimento, disponibilizando relatórios sobre o que foi acessado e quem o acessou e qual o nível de perigo que traz a rede. Conta também com um sistema de segurança de políticas de acesso completo com o controle do conteúdo que se pode acessar na internet dentro da rede da empresa.

O Firewall XG conta com um Sistema de Prevenção de Intrusão (IPS), que examina o tráfego de tudo que é acessado na rede com o objetivo de detectar e impedir as explorações das vulnerabilidades no sistema. Outra ferramenta que o Firewall XG oferece é o Advanced Threat Protection (ATP), responsável por tentar capturar e identificar estações de trabalho comprometidas por ameaças avançadas que tenham passado dispersos pela segurança da rede, ao detectar o tráfego com o perfil de tentativas de invasão, ou estações que tentam (SOPHOS, 2017).

Diante dos recursos providos por esta ferramenta, foi realizado um comparativo em uma empresa X, sobre a diferença do consumo de internet antes e depois das implementações de segurança e políticas de acesso no Firewall, sendo monitorado quais foram as aplicações e as categorias de acesso. No primeiro momento o Firewall ficou apenas em modo bridge e recolhendo as informações do que se era acessado, sem haver a implementação de nenhuma política de acesso.

Em um segundo momento foi aplicado às políticas de acesso, bloqueando sites como Facebook, Instagram, jogos online e outros conteúdos que não eram considerados produtivos para o horário e local de trabalho, apenas deixando liberado sites que não são produtivos em horários de intervalo e para pessoas específicas. A análise dos dados foi realizada utilizando o relatório desta, comparando quais foram os acessos antes e depois da aplicação de políticas de acesso no Firewall da Sophos XG que fica em funcionamento na rede da empresa.

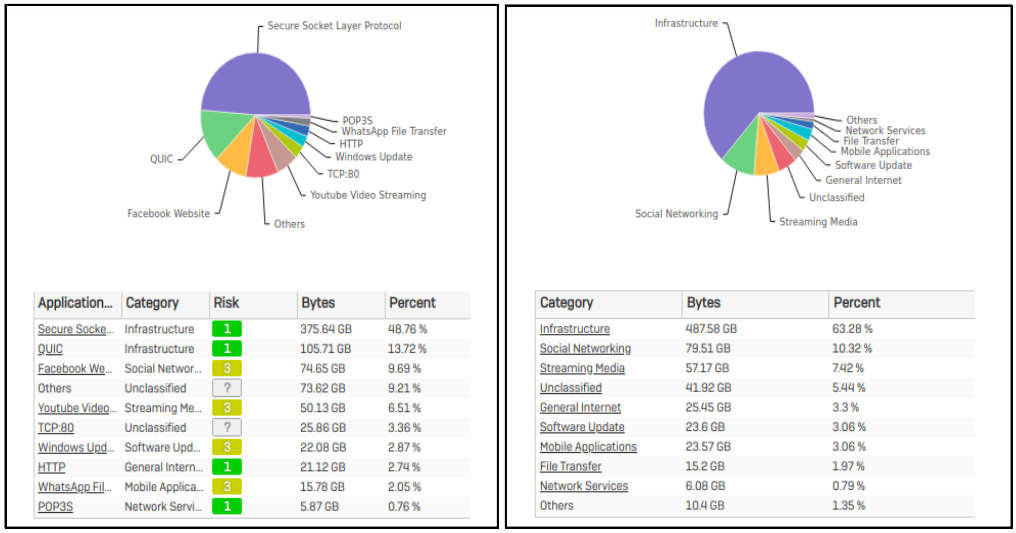
4. Resultados Parciais

A pesquisa baseou-se em um período de 30 dias, foram 15 dias com o firewall em modo bridge, onde ele apenas gerou relatórios do que estava sendo acessado na rede, sem fazer nenhum tipo de bloqueio. Após esse período foi aplicado as políticas de acesso,

definidas pelo gestor da empresa, após ter o relatório apresentado com as informações recolhidas pelo equipamento, foram aplicadas as políticas de bloqueios de aplicações, como Facebook, Instagram, YouTube. Porém, os bloqueios não foram feitos para toda a rede, mas sim parcialmente, definindo horários e também os usuários que poderiam acessar determinados conteúdos.

No primeiro relatório visto na Figura 1 pode se observar que o consumo de internet na empresa de conteúdo não produtivo era muito alto e foram aplicadas políticas baseadas nesses acessos, o período de teste ocorreu em um mês antes da implementação das políticas, abaixo podemos ver o acesso antes da aplicação das políticas. Tendo no primeiro gráfico as aplicações mais utilizadas na rede, e no segundo a classificação das categorias mais acessadas.

Figura 1 – Aplicações e categorias mais acessadas antes da ativação das políticas de acesso



Application...	Category	Risk	Bytes	Percent
Secure Socke...	Infrastructure	1	375.64 GB	48.76 %
QUIC	Infrastructure	1	105.71 GB	13.72 %
Facebook We...	Social Networ...	3	74.65 GB	9.69 %
Others	Unclassified	?	73.62 GB	9.21 %
Youtube Video...	Streaming Me...	3	50.13 GB	6.51 %
TCP:80	Unclassified	?	25.86 GB	3.36 %
Windows Upd...	Software Upd...	3	22.08 GB	2.87 %
HTTP	General Intern...	1	21.12 GB	2.74 %
WhatsApp Fil...	Mobile Applica...	3	15.78 GB	2.05 %
POP3S	Network Servi...	1	5.87 GB	0.76 %

Category	Bytes	Percent
Infrastructure	487.58 GB	63.28 %
Social Networking	79.51 GB	10.32 %
Streaming Media	57.17 GB	7.42 %
Unclassified	41.92 GB	5.44 %
General Internet	25.45 GB	3.3 %
Software Update	23.6 GB	3.06 %
Mobile Applications	23.57 GB	3.06 %
File Transfer	15.2 GB	1.97 %
Network Services	6.08 GB	0.79 %
Others	10.4 GB	1.35 %

Fonte: autores

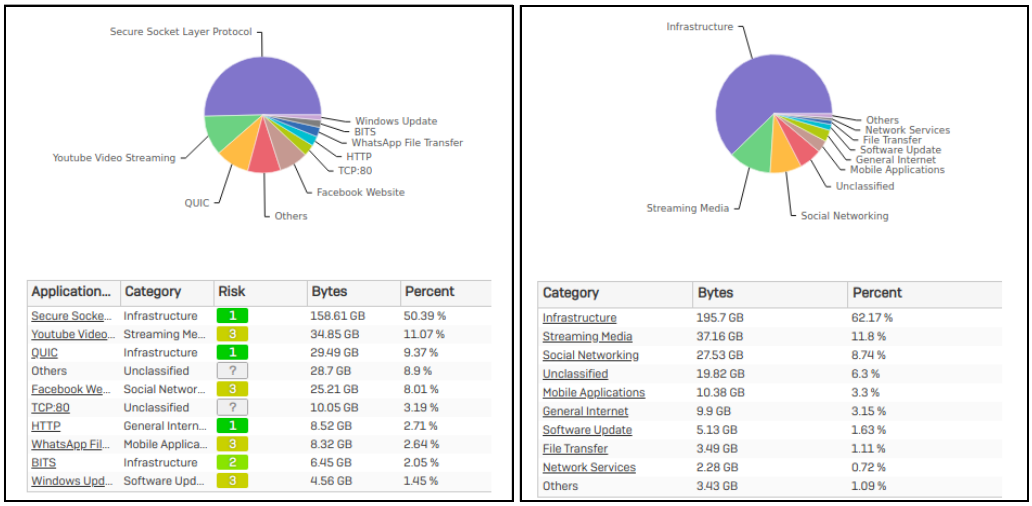
No primeiro gráfico é possível visualizar os aplicativos mais acessados na rede, que estiveram concentrados no Facebook, YouTube e transferência de arquivos de WhatsApp, o que pode não ser produtivo para a empresa, pois além de não produzir os colaboradores atrapalham o trabalho dos colegas consumindo a internet, seja acessando vídeos, ou redes sociais. Se torna importante destacar que existem funções e cargos em empresas que trabalham com este tipo de recurso e redes sociais, mas não foi o caso desta empresa. No segundo gráfico são mostradas as categorias mais acessadas na rede, o que se percebe é que a segunda categoria mais utilizada na empresa são as redes sociais, corroborando para o que foi constatado no primeiro gráfico.

A partir deste ponto, as políticas de segurança foram implementadas na empresa. Redes sociais foram liberadas somente em horário de intervalo dos funcionários, e liberados para pessoas específicas, além de estabelecer o limite de banda ao acessar o YouTube e as redes sociais, para que o consumo desses acessos não viesse a afetar o andamento do trabalho.

Um novo relatório foi gerado após um mês desta implementação, onde é possível observar que o uso da internet de conteúdo impróprio na empresa diminuiu consideravelmente. Vale ressaltar que algumas categorias improdutivas, foram liberadas em específico para algumas pessoas, e também em horários onde os colaboradores

podem acessar, determinado pelo gerente da empresa. A Figura 2 apresenta os gráficos descritos.

Figura 2 – Aplicações e categorias mais acessadas após a ativação das políticas de acesso



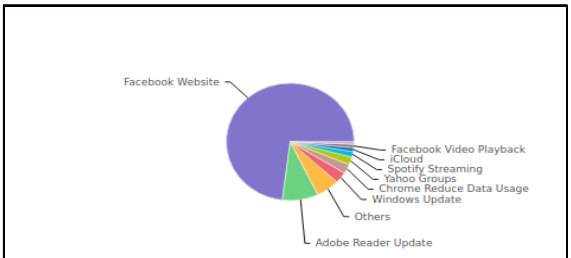
Application...	Category	Risk	Bytes	Percent
Secure Socke...	Infrastructure	1	158.61 GB	50.39 %
Youtube Video...	Streaming Me...	3	34.85 GB	11.07 %
QUIC	Infrastructure	1	29.49 GB	9.37 %
Others	Unclassified	?	28.7 GB	8.9 %
Facebook We...	Social Networ...	3	25.21 GB	8.01 %
TCP:80	Unclassified	?	10.05 GB	3.19 %
HTTP	General Intern...	1	8.52 GB	2.71 %
WhatsApp Fil...	Mobile Applica...	3	8.32 GB	2.64 %
BITS	Infrastructure	2	6.45 GB	2.05 %
Windows Upd...	Software Upd...	3	4.56 GB	1.45 %

Category	Bytes	Percent
Infrastructure	195.7 GB	62.17 %
Streaming Media	37.16 GB	11.8 %
Social Networking	27.53 GB	8.74 %
Unclassified	19.82 GB	6.3 %
Mobile Applications	10.38 GB	3.3 %
General Internet	9.9 GB	3.15 %
Software Update	5.13 GB	1.63 %
File Transfer	3.49 GB	1.11 %
Network Services	2.28 GB	0.72 %
Others	3.43 GB	1.09 %

Fonte: autores

O primeiro gráfico mostra as aplicações mais acessadas, em que, foi possível perceber que o consumo aos acessos de Facebook, YouTube e transferências de WhatsApp diminuíram perceptivelmente. O consumo gasto com o conteúdo produtivo aumentou na categoria de Infraestrutura, sendo mais do que 60% do que é utilizado na rede. Também foi gerado um gráfico das aplicações mais bloqueadas durante todo o período de uso da ferramenta, conforme Figura 3.

Figura 3 – Aplicações mais bloqueadas durante todo o período



Application...	Category	Risk	Hits	Percent
Facebook We...	Social Networ...	3	597272	73.04 %
Adobe Reader...	Software Upd...	2	74297	9.09 %
Others	Unclassified	?	48407	5.87 %
Windows Upd...	Software Upd...	3	24895	3.04 %
Chrome Redu...	Proxy and Tun...	5	21128	2.58 %
Yahoo Groups	Social Networ...	2	17484	2.14 %
Spotify Strea...	Streaming Me...	2	12346	1.51 %
iCloud	File Transfer	3	8745	1.07 %
Facebook Vid...	Streaming Me...	2	7640	0.93 %
Twitter Website	Social Networ...	3	5470	0.67 %

Fonte: autores

O gráfico anterior mostra que o Facebook é o aplicativo que mais se tenta acessar, e que o firewall nega o acesso, somando mais de 70% dos bloqueios da rede. Assim, ao analisar os resultados obtidos é possível ver que o tempo ocioso dos colaboradores não produzindo no tempo de trabalho era muito grande, e que ao utilizar

o Firewall da Sophos, o consumo de sites não produtivos diminuiu, pois ao aplicar as políticas de acesso, os sites acessados ficaram bloqueados para o horário de trabalho.

5. Considerações Finais

A informação cada vez mais é considerada o elemento mais valioso de uma empresa, o que exige também uma atenção centralizada e dedicada à sua proteção. O uso de ferramentas para realizar este processo pode auxiliar a diminuir os riscos inerentes. No trabalho realizado, foi possível verificar que o Firewall XG da Sophos é uma relevante opção para a segurança de uma rede empresarial.

No contexto deste trabalho, também foi possível averiguar que ela pode auxiliar e contribuir para o resultado produtivo de uma empresa, pois com as políticas bem aplicadas se tem o melhor uso da internet e também faz com que os colaboradores tenham acesso somente a sites e aplicativos de produção em seu horário de trabalho, passando menos tempo dispersos navegando na internet.

A utilização do XG SOPHOS auxilia o gerenciamento da segurança da informação, como criar e gerenciar políticas de acesso, redirecionamentos, consultar relatórios de consumo, páginas mais acessadas, além de evitar que pessoas não autorizadas usem a conexão do ambiente para acesso à internet. Como sugestão para trabalhos futuros, uma análise comparativa entre várias soluções de firewalls de nova geração, incluído a solução utilizada neste trabalho, se torna válida.

Referências Bibliográficas

Bär, H. (2017). 4 vulnerabilidades que mais afetam a segurança da informação. Disponivel em: https://triplait.com/4-vulnerabilidades-que-mais-afetam-a-seguranca-da-informacao. Acesso em: 25/05/2019.

Carvalho, G. M. (2018). Diagnóstico de gestão da segurança da informação em empresas nacionais do setor financeiro. Trabalho de conclusão de curso, Departamento de Ciências Administrativas, UFRGS, 76 p.

Ferreira, M. R.; Dolci, D. B.; Tondolo, V. A. G. (2016). Uma Proposta de Diagnóstico e Autoavaliação da Gestão da Segurança da Informação. XL Encontro da ANPAD,.

Kurose, J. F. (2013). Redes de Computadores e a Internet: uma abordagem topdown. 6. ed. São Paulo: Editora Pearson.

NIC.BR. Disponível em: <http://www.nic.br/noticia/releases/cresce-uso-de-internet-e-redes-sociais-pormicroempresas-no-brasil-aponta-pesquisa-do-cetic-br/ >. Acesso em: 06 de junho de 2019.

Panes, G. G. (2011). Firewall Dinâmico: Uma implementação Cliente/Servidor. Dissertação de Mestrado, Pós-Graduação em Ciência da Computação, 72p.

Sophos XG. (2017). Disponível em: https://www.m3corp.com.br/sophos/sophos-utm-2. Acesso em: 26/06/2019

Sophos. (2017). Disponível em: <https://www.sophos.com/en-us.aspx. Acesso em: 26/06/2019

Turban, E.; Volonino, L. (2013). Tecnologia da Informação para Gestão: Em busca do melhor desempenho Estratégico e Operacional. 8ed. Porto Alegre: Bookman. 721 p.