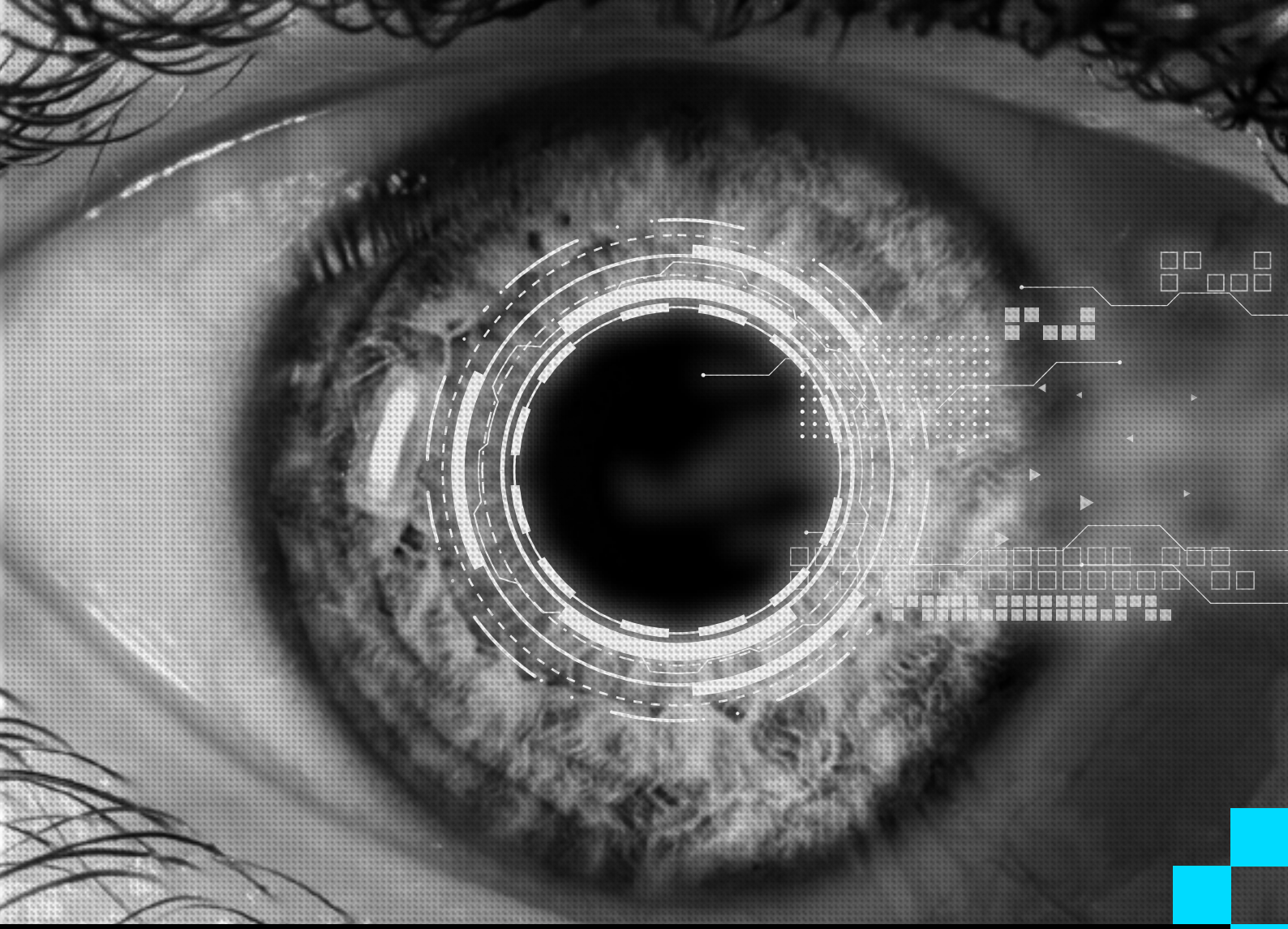


FILTRO DE CONTEÚDO WEB

ostec
Segurança digital de resultados

Gerir de maneira eficiente o uso da internet é um passo importante, que não somente aumenta a segurança do ambiente corporativo e das pessoas, mas promove ganhos de produtividade.

INTRODUÇÃO

A internet é composta por um universo de conteúdo que pode ser facilmente acessado, através dos mais variados dispositivos. O que no início era totalmente direcionado para fins militares e acadêmicos, atualmente ocupa a palma da mão de pessoas, nas mais variadas circunstâncias.

O acesso rápido à informação é um dos principais pontos positivos neste contexto, que inclui conteúdos relevantes dos mais variados tipos, assim como aplicações web que facilitam a gestão e execução de atividades, em meio corporativo.

A internet alterou o formato de operação de boa parte das empresas, contribuindo para o surgimento de novos negócios e para a extinção de outros. A intensificação do uso da internet, também motivou o início de discussões em torno do termo segurança da informação, que ganha força com as evoluções tecnológicas e da internet.

A quantidade de informações também inspira cuidados, uma vez que nem todo conteúdo disponível na rede é considerado lícito, correto, e para o mundo dos negócios, útil para acesso durante a jornada de trabalho.

Isso quer dizer que classificar o conteúdo de sites, que surgem aos milhares diariamente, para os mais variados fins, é uma atividade humanamente impossível sem contar com uma ferramenta que automatize esse processo.

Em outras palavras a internet trouxe inúmeros benefícios para as empresas, contudo seu uso inspira cuidados. Neste e-book apresentaremos conceito, funcionalidades e benefícios associados ao uso do filtro de conteúdo web, possibilitando que você identifique lacunas para utilização desta tecnologia em meio corporativo.

A PRODUTIVIDADE NA ERA DA INTERNET

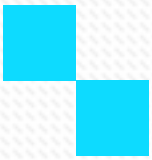
A distração, em um ambiente de trabalho que tenha acesso constante e irrestrito a internet, está a um clique de distância do colaborador, e isso pode representar perdas financeiras representativas para os negócios. Confira a **calculadora da produtividade**.

Neste sentido, as perdas são classificadas de duas formas: Desperdício de tempo, ocorrendo quando o colaborador aplica seu tempo no desenvolvimento de atividades não relacionadas ao escopo de trabalho. E a segunda forma, que está associada a falta de concentração/

foco, gerando falhas, muitas vezes graves, nas entregas dos colaboradores. Ambas formas trazem prejuízos representativos para os negócios, independentemente do seu segmento ou porte.

Por outro lado, dependendo do tipo de negócio e da geração de pessoas com quem está trabalhando, é preciso entender que restrições de uso a internet podem também afetar a motivação, e por consequência refletir negativamente na produtividade. O grande desafio, neste sentido, é identificar qual o perfil predominante em sua empresa, para poder tomar medidas pontuais, quando necessário.

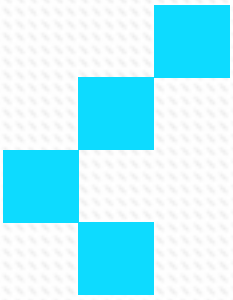
Em muitos casos, colaboradores reconhecem que usam a internet para fins pessoais durante o horário de trabalho, e justificam que tais atitudes estimulam a produtividade de maneira indireta. Infelizmente o equilíbro de todos, ou da maioria dos colaboradores, em um ambiente sem controle é algo bastante utópico, assim como os estudos que relatam ganho de produtividade associado as fugas utilizando a internet.



Em estruturas organizacionais onde há uma gestão baseada em metas e resultados muitas pessoas não se preocupam com a distração ou até mesmo acesso inadequado à internet para fins pessoais, desde que entreguem o resultado. É uma visão que vale reflexão, pois o rendimento do colaborador poderia ser superior, assim como o acordo de metas e resultados poderia ser mais apertado, trazendo benefícios para o negócio,

principalmente em momentos de crise e mão de obra escassa.

A percepção de problemas relacionados a produtividade, em um ambiente corporativo, assim como a definição de estratégias para superar estes problemas, é algo que exige elevado grau de sensibilidade e acompanhamento do time de recursos humanos, bem como dos responsáveis por cada setor, para acordar o que é considerado adequado para o negócio, o perfil das pessoas e o modelo de gestão.



É também importante que as regras definidas nesse contexto sejam discutidas e acordadas não somente em um modelo top-down, do contrário, a possibilidade de sabotagem, por parte do colaborador é muito grande.

Neste sentido, vale a pena ressaltar que não há uma receita a ser aplicada, para potencializar o uso da internet em ambientes corporativos, incrementando a produtividade e motivação dos colaboradores. Por conta disso, ferramentas que oferecem flexibilidade de controle, e visibilidade dos acessos para os gestores, são primordiais para enfrentar os desafios, fazendo com que o negócio, como um todo, seja beneficiado.

PROBLEMAS NÃO CONHECIDOS DE SEGURANÇA

Os usuários da internet, em sua maioria, não conhecem os riscos associados ao uso indiscriminado do recurso. Os riscos mais conhecidos, são aqueles considerados comuns, de fácil identificação, tal como alguns tipos recebidos por e-mail. Vale ressaltar que mesmo conhecendo as consequências, boa parte das causas e dos meios de infecção, são desconhecidos.

O fator a ser entendido é que, diferentemente de anos atrás, hoje a estrutura de phishing, e técnicas similares, que visam enganar o usuário para obter suas informações, é baseada no envio de links, que normalmente apontam para páginas na internet, onde há um conteúdo malicioso.

Por mais atualizado que um sistema operacional e antivírus esteja, trabalhar em uma estrutura multicamada

de segurança, é algo essencial para as organizações, dada a necessidade cada vez mais constante de proteção dos ambientes computacionais.

Nesse sentido, uma camada de proteção que não esteja no equipamento dos colaboradores, mas no perímetro da organização, pode minimizar estes problemas mesmo diante de alguma negligência ou descuido dos usuários.

Possuir um acesso à internet totalmente liberado para os colaboradores, ou bloquear somente aquilo que se conhece, é um risco potencial de que, diante de um phising bem elaborado ou algo similar, o usuário realmente acabe sendo comprometido, por mais conhecimento que este possua.

Isso não significa, para a maioria dos negócios, que tudo deva ser bloqueado com o intuito de evitar tais problemas, pois se isso for feito, pode haver reflexos negativos relacionados a produtividade e motivação dos colaboradores, que estarão mais engessados para desempenhar suas funções.

Novamente o equilíbrio oferecido por uma solução que permita gerenciar estes eventos de maneira adequada, afetando o mínimo possível a operação e experiência dos usuários, é fator de sucesso para as organizações que hoje dependem da internet para suas atividades.

FILTRO DE CONTEÚDO WEB

Um filtro de conteúdo web, ou somente proxy web, é uma solução muito interessante para os problemas que foram caracterizados, pois são posicionados de maneira estratégica entre as redes internas (ou protegidas) e as saídas para a internet.

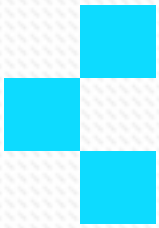
Desta forma, os equipamentos dentro de uma rede não têm acesso direto à internet sem passar por esse dispositivo de segurança, que irá regular e normalizar o acesso de acordo com as políticas do negócio.

Existem diversas soluções de proxy ou filtro de conteúdo web, a diferença basicamente consiste na flexibilidade em criar as regras de acesso, integração com estruturas de terceiro como autenticação, antivírus e outros, bem como bases prévias de conhecimento de URLs, que são comumente chamadas no mercado como categorias.

Uma tecnologia bastante comum aplicada em proxy web é o conceito de caching, o que causa a sensação de aceleração da internet para alguns acessos. O caching pode ser utilizado em memória ou dispositivo de armazenamento secundário, e basicamente consiste em guardar em um determinado espaço configurado, os objetos que são mais acessados.

Isso garante que diante de muitas requisições para um determinado destino, o proxy não precisa ir na internet descarregar a informação, podendo realizar esta atividade localmente, e em alta velocidade para o requerente, tendo em vista que o objeto encontra-se em memória. Isso pode, em muitos casos, gerar uma grande economia de banda e, portanto, é um recurso a ser avaliado durante o processo de aquisição.

Além destes pontos é importante que as tecnologias ofereçam um nível de report (relatório) interessante para o time de tecnologia ou até mesmo outras gerências, através de dashboard, estatísticas de uso, relatórios automáticos e outros que ofereçam não somente conhecer o tráfego utilizado, mas também interagir com o mesmo ao longo do tempo, garantindo conformidade do ambiente.



Basicamente um proxy web consiste em um conjunto de objetos (em muitos casos chamados ou identificados como listas de acesso ou ACLs), com determinados conteúdos, que podem ser associados a uma determinada regra, que deverá liberar ou bloquear o tráfego ou requisição de um dispositivo.

Em outras palavras, um proxy permite combinar listas de acesso de tipos variados (horários, usuários, sites etc), para a criação de regras que visam controlar o uso da internet. Isso possibilita, por exemplo, estabelecer que determinado usuário poderá acessar a lista de sites permitidos, dentro de um intervalo de horário, estabelecido pela empresa.

UM POUCO SOBRE ARQUITETURAS DE PROXY

Um proxy web precisa estar estrategicamente posicionado em uma topologia de rede para que possa desempenhar sua função, ou, em outros casos onde ele está em paralelo a infraestrutura, outros recursos precisam garantir que somente após o usuário passar por ele é que o acesso será liberado para a internet.

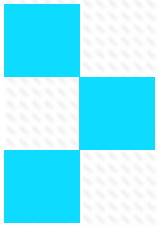
Em muitas soluções o proxy web apresenta-se como um recurso presente em um ativo de segurança mais complexo, como por exemplo um Firewall/ UTM ou NGFW e, portanto, está atuando diretamente no gateway. Em outras arquiteturas o mesmo é um software, appliance ou virtual appliance dedicado, somente a essa função.

Neste último caso é importante garantir que os usuários passarão suas requisições web primeiramente para o

proxy, neste sentido é possível criar regras para liberar somente o tráfego web gerado pelo proxy, ou ainda criar políticas de controlador de domínio para definir o proxy, entre outras possibilidades.

Quanto a utilização de proxy dedicado ou associado a soluções de UTM, não existem orientações formalizando boas práticas de conduta. Atualmente as soluções de firewall estão com recursos altamente avançados de proxy, o que garante features similares, iguais ou superiores a soluções dedicadas de proxy.

O aspecto de usar uma estrutura dedicada para o proxy está muito mais relacionado a necessidade do ambiente em termos de escalabilidade, do que necessariamente em atender uma premissa de segurança. Você deve analisar aquilo que está mais adequado a sua necessidade e seu ambiente.



CONTROLE BASEADO EM CATEGORIAS

Com o passar dos anos, gerenciar a quantidade de sites existentes na internet tornou-se um desafio impossível de ser superado por empresas de maneira geral. Por conta disso, surgiram empresas especializadas em categorizar a internet e oferecer as bases de dados segmentadas em categorias, para serem utilizadas em soluções de segurança.

O controle baseado em categorias é um recurso opcional em muitas soluções de proxy web, e que oportuniza o analista de segurança/gestor trabalhar com regras baseadas em grupos de interesse ou temas, facilitando a personalização do uso da internet, flexibilizando necessidades de setores e pessoas, sem ferir aspectos de segurança.

Um erro comum de muitos negócios é oferecer acesso irrestrito para diretorias e gerências, além de não ser um bom exemplo de política dentro da empresa, tal atitude pode gerar problemas associados a infecção de ativos de rede, que podem se espalhar por toda a estrutura corporativa.

Isso porque ao liberar todo o acesso, bilhões de sites de conteúdo ilícito, que visam comprometer usuários, passam a ter acesso totalmente liberado. Ao aplicar este tipo de política, a empresa corre grande risco de colocar em cheque todas as diretrizes de segurança, desenvolvidas para proteger o negócio.

Com a aplicação do módulo de categorização de conteúdo, é possível liberar os acessos de dirigentes e gestores, restringindo apenas sites classificados em categorias do tipo malware, hacking, cracking, warez e outros conteúdos que podem impactar negativamente no negócio.

As categorias, portanto, permitem que você personalize o uso da internet de maneira mais eficiente, complementando as listas de acesso de sites produzidas manualmente, utilizadas com finalidade específica.

MODOS DE UTILIZAÇÃO: TRANSPARENTE, MANUAL OU AUTOMÁTICO?

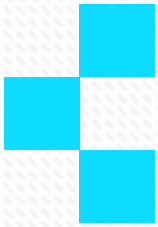
Existem algumas formas de trabalhar com proxies, muitos deles suportam o recurso de transparência, que permite que o firewall ou outro dispositivo intercepte o tráfego HTTP e encaminhe para o endereço e porta em que o serviço de proxy está operando.

Esse modelo parece muito interessante porque não envolve nenhuma necessidade de intervenção no dispositivo dos usuários, no entanto, ele possui um conjunto de outras dificuldades estruturais que inviabilizam seu uso em um ambiente corporativo onde o o objetivo principal é controle.

Muitas aplicações web foram construídas e a grande maioria delas utiliza uma conexão segura (HTTPS), isso dificulta a transparência tendo em vista que a intercepção SSL transparente é um grande desafio. Além disso, existem outras aplicações baseadas no protocolo HTTP que usam diferentes portas, e neste caso, prever isso dentro de um cenário dinâmico para criar o redirecionamento transparente é algo com pouca probabilidade de funcionamento e eficiência.

Por conta disso algumas outras alternativas podem ser utilizadas, a primeira e mais rápida é chamada de proxy manual, onde a definição de proxy é realizada diretamente no navegador, aplicação ou sistema operacional. O usuário pode realizar essa configuração (do contrário terá acesso completamente restrito) ou o processo pode ser automatizado.

Em estruturas que possuem um controlador de domínio ou solução similar que suporte configuração das diretivas de segurança, de maneira centralizada, o mesmo deve ser utilizado para replicação das configurações, sendo estas aplicadas, efetivamente, no momento do logon do usuário no sistema operacional.



Para finalizar, existe um terceiro modelo que tem bastante aderência em diversas organizações, que é chamado de WPAD. Neste formato, ativado através do recurso de detecção automática de proxy, o sistema operacional ou navegador tenta localizar o arquivo com as diretivas de conexão da rede, e caso não encontre, nenhuma configuração é aplicada.

Esse modelo é interessante, pois permite que a mesma configuração possa ser aplicada em um dispositivo que sofre mudança de local, diferentemente do caso do proxy manual, onde o equipamento, mesmo fora da empresa, vai tentar fazer a conexão com o proxy configurado, impossibilitando a navegação, a não ser que a mesma for feita através de uma VPN.

As maiores dificuldades de uso do WPAD, no entanto, estão associadas a dispositivos móveis. Isso não se dá

por uma limitação do formato, mas sim das aplicações e sistemas operacionais móveis, que não carregam corretamente informações de outros protocolos além do HTTP, fazendo com que tráfego HTTPS, por exemplo, passe por fora do proxy e seja bloqueado.

Não existe uma melhor forma de utilizar, cada empresa deve avaliar dentro da sua necessidade e ambiente aquele formato que mais se adaptará ao ambiente. O importante é que os usuários passem pelo proxy, garantindo a segurança corporativa.

A IMPORTÂNCIA DOS REGISTROS E AUDITORIA

Um dos recursos fundamentais do proxy é manter o registro dos acessos que são realizados para a internet. Isso é importante por vários motivos, podendo ser aplicado no início da implantação de projetos de segurança, para melhor entendimento do comportamento e perfil de uso da internet, servindo como base para a construção de políticas, assim como necessidades de auditoria, para os mais variados fins.

Conhecer aquilo que é mais utilizado por toda a empresa, por usuários, ter uma visão de setores, sites que são mais acessados, períodos em que há maior acesso, tudo isso é fundamental para facilitar a tomada de decisão e a construção de uma política de acesso.

Os relatórios também podem ser uma fonte muito interessante para gestores de equipes avaliarem o desempenho dos colaboradores. Verificar quais as principais atividades dos times na internet, para identificar desvios de conduta pode ser uma boa oportunidade para aprimorar o desempenho das equipes.

Com relação ao armazenamento dos relatórios de navegação dos usuários é importante verificar o tempo de retenção, demandado pela estrutura corporativa, a fim de definir a solução mais adequada para aquisição. Se você tem um alto volume de dados e muitos usuários, é comum que seja necessário alocar uma quantidade maior de espaço para armazenamento dos relatórios e logs de navegação.

Gravar o histórico de navegação dos usuários pode ser decisivo no processo de elucidação de fatos ocorridos no passado. Esse registro, em alguns casos, também oferece conformidade com o Marco Civil, caso seja necessário fornecer alguma informação para entidades legais.

Se sua empresa oferece acesso wifi para visitantes, fornecedores e outras pessoas que circulam no ambiente corporativo, sem possuir vínculo com o negócio, é muito prudente armazenar estes registros, assim como deixar as regras de acesso claras, através da apresentação de termo de uso para os indivíduos que utilizarem a estrutura.

INTEGRAÇÕES COM SOLUÇÕES DE TERCEIROS

É comum que soluções de proxy possuam integrações com outros produtos para incrementar seus recursos, como por exemplo integração com antivírus corporativos.

O protocolo comumente utilizado para esse propósito chama-se ICAP e oferece uma grande flexibilidade para o proxy ser integrado com outras soluções, podendo torná-lo mais robusto em seu propósito.

Além disso, cada fornecedor mantém uma lista de possibilidades de integração de suas soluções com ferramentas ou produtos de terceiros com o mesmo propósito de incrementar recursos e por consequência oferecer um produto mais completo e eficiente.

Antes de adquirir uma solução, identifique claramente qual é o problema a ser resolvido, e quando tiver a certeza que uma solução de proxy e suas possibilidades é a resposta, busque no mercado uma solução que entregue produto e serviço adequado a necessidade de seu negócio.

CONTINUE LENDO

SE VOCÊ GOSTOU DO ASSUNTO E GOSTARIA DE NOVAS LEITURAS, FIQUE A VONTADE PARA CONSULTAR ATRAVÉS DOS LINKS ABAIXO TEMAS RELACIONADOS EM NOSSO PORTAL.

VOCÊ SE INTERESSOU PELO CONTEÚDO?

ESCLAREÇA SUAS DÚVIDAS COM ESPECIALISTAS NO ASSUNTO

CONVERSE COM ESPECIALISTA

facebook.com/ostec

linkedin.com/company/ostec-business-security

contato@ostec.com.br

www.ostec.com.br

ostec.blog

ostec

Segurança digital de resultados