COMO A SEGURANÇA DA INFORMAÇÃO INFLUENCIA NA PRODUTIVIDADE DA SUA SERVENTIA

GT
Soluções em TI

Sumário

1 - ACESSAR A INTERNET COM SEGURANÇA E MANTER A PRODUTIVIDADE NO DIA A DIA 1

2 - COMO O MONITORAMENTO DE REDE CONTÍNUO PODE AUMENTAR A SUA COMPETITIVIDADE ... 4

O QUE É MONITORAMENTO DE REDE CONTÍNUO? 4
ENTÃO, QUAL A IMPORTÂNCIA DO MONITORAMENTO DE REDE CONTÍNUO? 6

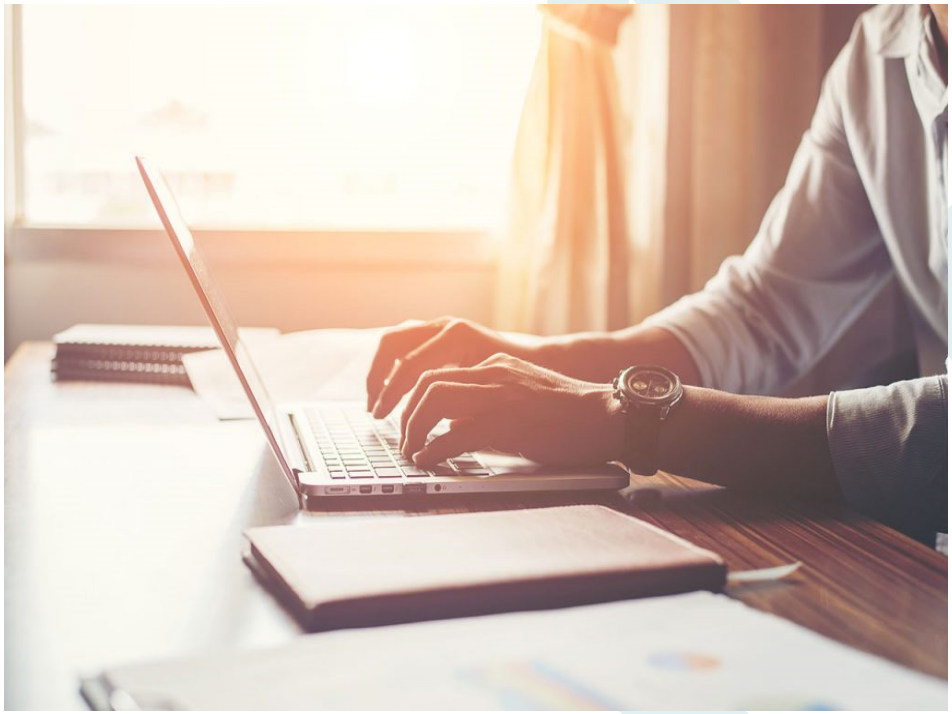
3 - 5 DICAS DE SEGURANÇA QUE AUMENTARÃO A PRODUTIVIDADE DA SUA SERVENTIA 7

1 – CRIE POLÍTICAS DE SEGURANÇA: 7
2 – LOCALIZE VULNERABILIDADES: 8
3 – UTILIZE FERRAMENTAS DE DEFESA: 8
4 – EDUQUE A SUA EQUIPE: 9
5 – FAÇA BACKUPS FREQUENTES: 9

4 - SERVIÇOS GERENCIADOS: COMO SUA SERVENTIA PODE SE BENEFICIAR 10

UM RESUMO RELEVANTE DAS VANTAGENS DE ADOÇÃO DOS NOSSOS SERVIÇOS GERENCIADOS PELA SUA SERVENTIA: 12

1 - Acessar a Internet com Segurança e Manter a Produtividade no Dia a Dia



Atualmente para qualquer profissional é impensável trabalhar sem acessar à internet durante a jornada de trabalho. Acessar a internet com segurança e manter produtividade no dia a dia das serventias vem sendo uma das maiores dores de cabeça na área de tecnologia para os departamentos de TI.

Ao mesmo tempo que a internet contribui para a geração de negócios ou no desenvolvimento das tarefas do dia a dia, o mau uso dessa ferramenta pode gerar problemas e até mesmo prejuízo para as serventias, principalmente envolvendo falhas de segurança como perda de dados ou influenciando negativamente na produtividade da equipe, com o desperdício de tempo e redução de foco nas tarefas.

Algumas pesquisas apontam que o tempo desperdiçado pelos colaboradores na internet pode chegar a 30% durante o trabalho. Já as despesas com falhas de segurança aumentaram 35%.

Diante deste cenário é vital para as serventias que os diretores e gestores de TI monitorem a produtividade da equipe e implementem políticas de utilização da internet, com soluções que permitam definir o que pode ou não ser acessado e que protejam os usuários do acesso a sites nocivos.

A gestão do acesso à internet gera inúmeros benefícios para as serventias:

- Segurança e proteção contra ameaças na internet;
- Menor risco de perda de informações e problemas com vírus;
- Redução de desperdício de tempo na internet pela equipe;
- Aumento da produtividade, qualidade e foco nas tarefas;
- Redução de despesas com manutenção de equipamentos;
- Informações e dados sobre o uso da internet;
- Melhoria no desempenho da rede, sistemas e recursos de tecnologia;

Existem diferentes soluções disponíveis no mercado para o gerenciamento do acesso à internet, porém, demandam alto investimento, envolvimento de profissionais técnicos especializados e exigem constante manutenção, atualizações e suporte. Isso faz com que essas soluções se tornem caras e muitas vezes inviáveis, principalmente para pequenas e médias serventias.

Com o propósito de preencher essa lacuna no mercado e oferecer uma solução acessível e simplificada às serventias de pequeno e médio porte a GT Soluções em TI disponibiliza o serviço de Controle de Acesso e Segurança Web Protection.

A solução de controle de acesso e segurança Web Protection da GT Soluções em TI está baseada em Cloud Computing, não existe necessidade de investimentos em Hardware e Software. Garanta a segurança em toda a sua rede em poucos minutos e sem custos extras.

Não importa o tamanho da sua serventia, a solução é configurável para qualquer tipo de ambiente, independentemente do número de equipamentos.

Veja algumas das principais características e vantagens da nossa solução de Controle de Acesso e Segurança Web Protection e solicite uma demonstração.

2 - Como o Monitoramento de Rede Contínuo Pode Aumentar a Sua Competitividade

O que é Monitoramento de Rede Contínuo?

O termo monitoramento de rede pode ter diversas interpretações, incluindo escaneamento de vulnerabilidades, captura de pacotes e análise, depuração de rede bem como os sistemas de automação de gerenciamento entre outros.

A fim de simplificar neste artigo, em termos de serviços gerenciados, vamos convencionar que monitoramento de rede significa fornecer subsídios que possibilitem observar e melhorar as condições da rede e da operação.

Simplificando, monitoramento de rede contínuo é saber o que está ocorrendo em sua rede, onde e quando está ocorrendo, por que está ocorrendo e se o que está sendo observado é motivo para preocupação ou não. Isso tudo a qualquer momento (24 X 7) e de qualquer lugar.

Em conjunto com outras soluções importantes, o monitoramento de rede contínuo é um elemento chave na detecção e prevenção de incidentes de segurança.

Você já observou quantos novos dispositivos passaram a usar a infraestrutura de rede? Celulares seus, dos funcionários, dos representantes comerciais, notebooks, impressoras com placa de rede, e essa variedade de dispositivos só tende a aumentar.

Imagine o seguinte cenário:

É muito comum uma intrusão de rede que se inicia quando um usuário clica em um link suspeito, ou arquivo recebido por email. Então, depois de dias ou até semanas, informações sigilosas da sua serventia são extraviadas. Somente depois de meses que o gestor identifica que uma intrusão aconteceu.

O Monitoramento de Rede Contínuo poderia ter evitado o incidente.

Neste caso, o monitoramento de rede contínuo poderia dificultar o ataque em diferentes momentos. Dessa forma seria possível detectar o acesso não autorizado nos momentos iniciais ao identificar links maliciosos em um email ou em um site acessado pelo usuário.

Adicionalmente como uma outra camada de segurança, quando um link malicioso é clicado o monitoramento contínuo de HTTP poderia bloquear a conexão para o servidor malicioso. Quando as informações sigilosas estão sendo extraviadas da rede, um monitoramento de rede na camada 3 poderia emitir um alerta e bloquear esse envio de dados.

O Monitoramento de rede contínuo tem como objetivo a melhoria constante de desempenho e confiabilidade de toda a sua infraestrutura como impressoras, switches etc. Isto possibilita um ponto único de contato para coordenar de forma proativa todas as atividades de gerenciamento.

Podemos dizer que o monitoramento de contínuo permite aos responsáveis pela segurança das informações da sua serventia analisar o contexto de cada pacote que entra e sai da rede corporativa. De forma que eles possam rapidamente reconhecer e diferenciar operações rotineiras de rede de comportamentos suspeitos e atividade não esperada.

Então, qual a importância do monitoramento de rede contínuo?

Não adianta ter as melhores soluções de segurança de email ou de controle de acesso à internet em sua infraestrutura se você não entende o que está ocorrendo. O monitoramento de rede contínuo é essencial para que você tenha visibilidade e conquiste essa compreensão.

Conhecendo bem sua rede, sabendo o que está ocorrendo, como e quando, será muito mais fácil garantir o melhor funcionamento dos demais recursos e soluções de segurança em sua rede corporativa minimizando os riscos de falhas de segurança.

3 - 5 Dicas de segurança que aumentarão a produtividade da sua serventia

Nos últimos anos, a cada dia aumenta a quantidade de dispositivos que se conectam de uma forma ou de outra à sua rede corporativa, seja local ou remotamente. E com isso aumenta também as chances de vulnerabilidades. E uma rede “atacada” pode geram uma série problemas que podem acarretar em perda de produtividade por motivos que vão desde lentidão da rede até dispositivos (computadores de laptops) em manutenção.

Abaixo listamos algumas pequenas atitudes que podem evitar que a sua serventia sofra comestes problemas:

1 – Crie políticas de segurança:

Políticas de segurança são uma série de orientações para os responsáveis pela segurança das informações da sua serventia. É um documento que deve conter um conjunto de normas, métodos e procedimentos, os quais devem ser comunicados a todos os funcionários, bem como analisado e revisado criticamente, em intervalos regulares ou quando mudanças se fizerem necessárias.

Hoje em dia a utilização da tecnologia e internet faz parte do cotidiano dos colaboradores no ambiente de trabalho, com o uso dos computadores, smartphones, sistemas gerenciais, e-mails, navegação na internet e tantas outras atividades.

Como a tecnologia e a internet são muito amplas e estão tão presentes, é necessário definir de que forma esses recursos podem ser usados no ambiente de trabalho. Por exemplo, usar um pendrive pessoal com vírus na serventia pode contaminar toda a rede

2 – Localize vulnerabilidades:

Para construir uma política de segurança sólida e eficiente, é necessário conhecer todo o ambiente da sua rede e listar quais possíveis falhas podem expor informações da sua serventia bem como dos seus clientes. Essas vulnerabilidades podem ser desde um software desatualizado até um celular não conhecido acessando rede wi-fi.

Muitas dessas vulnerabilidades podem parecer inofensivas e por isso mesmo são as mais frequentes.

Existem ferramentas, softwares que podem realizar um diagnóstico de toda a sua rede, listando desde sistema operacional com atualização pendente até senhas inseguras, mas uma verificação manual também pode ajudar muito.

3 – Utilize ferramentas de defesa:

A adoção de ferramentas de defesa como antivírus, firewall etc. são de extrema importância para detectar, e na grande maioria dos casos, resolver problemas de segurança. Utilize estas ferramentas para monitorar tráfego, detectar invasões, escanear emails, restringir acesso a sites maliciosos, etc.

Além disso, todos sabemos que os softwares de segurança pedem regularmente atualizações, mas nem todos as fazem. Isso traz riscos? Sim, e você nem imagina o quanto.

Segundo a ABRANET, 92% das vulnerabilidades críticas de infraestrutura de redes e sistemas em serventias brasileiras detectadas no ano passado estavam diretamente relacionadas a ausência de atualização de programas.

4 – Eduque a sua equipe:

Softwares de segurança não são a solução definitiva. Seus funcionários precisam fazer a parte deles. É muito importante educá-los acerca do uso consciente dos recursos de tecnologia da sua serventia. A maioria dos ataques maliciosos explora o desconhecimento dos usuários.

Converse com os funcionários ou colegas sobre a importância de usar email corporativo somente para fins corporativos. Além de questões relacionadas à segurança, o uso de emails corporativos para fins pessoais com o tempo acabará afetando também a produtividade da sua equipe.

5 – Faça backups frequentes:

O backup é um importante meio para manter as informações da sua serventia em segurança. Com uma política de backup eficiente, sua serventia não corre o risco de perder informações importantes. Como mais uma medida de segurança criptografe seus backups.

Mantenha sempre várias cópias em mídias diferentes e em locais físicos diferentes. Manter várias cópias de todos os dados da serventia é fundamental. Tente imaginar sua serventia sofrer algum tipo de ataque ou perder todos dados corporativos de alguma forma (planilhas, banco de dados de sistemas, dados de cliente e vendas, e-mails etc.), com certeza os prejuízos são imensos.

Todos os dias surgem e continuarão a surgir novas técnicas e recursos para um ataque mal-intencionado à sua serventia. Para evitar prejuízos é muito importante que as políticas de segurança das informações contemplem os diversos níveis, cada nível de segurança dificulta o trabalho do invasor. Os serviços gerenciados da GT Soluções em TI contemplam todas as camadas de segurança, desde AntiSpam e antivírus até soluções de backup e Segurança de servidores.

4 - Serviços Gerenciados: Como sua Serventia Pode se Beneficiar

Em tempos de inúmeras ameaças digitais e de diversas categorias (vírus, ransomwares, adwares etc.), as pequenas e médias serventias (PME) podem ser as maiores prejudicadas em termos de proteção ativa. Em geral, frente aos diversos investimentos necessários para impulsionar os negócios, os investimentos em segurança da informação frequentemente ficam em segundo plano. Neste sentido a GT Soluções em TI traz para o mercado o seu pacote de Serviços Gerenciados, que vem para flexibilizar custos e resolver seus problemas de segurança.

No entanto, não faltam motivos para que sua serventia comece a pensar em segurança das informações como fator estratégico que habilita e mantém o funcionamento de seu negócio. Por exemplo, a maioria das serventias hoje, por menor porte que tenha, opera com o apoio de tecnologias. Para citar algumas poucas necessidades, as PMEs precisam:

- Garantir a disponibilidade de recursos de rede e dos links de internet;
- Proteger as comunicações que envolvam informações confidenciais como emails e documentos;
- Ter visibilidade sobre comportamento de usuários, aplicações utilizadas, sites navegados;

- Gerir usuários, seus acessos e privilégios;
- Monitorar como seus funcionários utilizam os recursos e sistemas;

Porém, para cada uma destas necessidades, há diferentes controles, existem diferentes camadas de segurança. Em muitos casos, as serventias de menor porte, não contam com assistência especializada de segurança, o que dificulta a escolha do produto correto para cada necessidade.

Neste contexto, a adoção de Serviços Gerenciados faz todo o sentido para a sua serventia independente do tamanho. Em termos de vantagens, o **custo-benefício** no formato oferecido pela GT fala mais alto, pois Nossos Serviços gerenciados reúnem diferentes tecnologias que a sua serventia precisa, com um investimento sob medida. Além disso, a **abrangência de camadas de proteção**, o **monitoramento constante da nossa equipe** e a **tomada de ações de forma proativa** são recursos chave dos nossos serviços.

Como fator técnico, vale considerar que a implantação dos Serviços Gerenciados corretamente planejados tem grande eficácia para identificar e reduzir as ameaças mais comuns do mundo digital, reduzindo os danos e os custos de incidentes de segurança. Para serventias menores o custo para se

recuperar de um incidente (seja um evento com malware, seja um sistema indisponível) pode ser muito maior do que investir preventivamente em controles de segurança. Este nível de eficiência pode ser alavancado com o bom alinhamento do produto com uma fonte constante de atualizações de inteligência, como é o caso dos Serviços Gerenciados da GT Soluções.

Um resumo relevante das vantagens de adoção dos nossos Serviços Gerenciados pela sua serventia:

- **Reduz o número de incidentes de segurança**, em função das diferentes tecnologias de proteção ativa que o produto integra nas diferentes camadas, como segurança para emails, monitoramento de rede e dispositivos, segurança para seus servidores etc;
- **Otimiza o investimento.** Sem considerar que o custo com diferentes tecnologias que trabalham em conjunto cai significativamente, os serviços gerenciados da GT permitem ainda reduzir infraestrutura pois você não precisa adquirir novos equipamentos. Ou seja, uma PME precisará de menos hardware de segurança, servidores e outros componentes;
- **Facilita a integração com novas funções.** Por sua natureza modular, os Serviços Gerenciados da GT Soluções podem facilitar a integração de novas capacidade de detecção e prevenção, elevando o nível de proteção dos ambientes que monitora. O mesmo princípio permite as serventias selecionar quais características de segurança habilitar;
- **Elimina a necessidade de uma equipe especializada dentro da sua serventia.** Todo o gerenciamento é realizado pela equipe da GT Soluções. Todo o serviço é totalmente transparente para você (estaremos o tempo todo ao seu lado e você nem perceberá J). Dessa forma sua serventia pode usar a experiência de seu time em outras funções estratégicas.

- **Automatiza diversas atividades rotineiras.** Manter todos os sistemas atualizados e funcionando corretamente, livrando-se de spams etc. consome muito tempo seu e da sua equipe. Os Serviços Gerenciados da GT Soluções forma concebidos para monitorar, gerir e atualizar seus diferentes módulos (como firewall, antimalware, sistema operacional etc.).
- **Melhora a performance da rede:** ao utilizar os Serviços Gerenciados da GT Soluções, os dispositivos da sua rede podem diminuir a sobrecarga sobre a mesma (visto que rotinas de atualizações verificação de vírus etc. podem ser executadas em horários de menor atividade como intervalos de almoço por exemplo) colaborando para melhorar a performance do ambiente. Assim, o produto pode também ajudar a reduzir a latência (o tempo que um pacote de dados percorre entre dois pontos), o que garante melhor desempenho dos sistemas e dispositivos utilizados pelo usuário.

Através dos Serviços Gerenciados da GT Soluções em TI, sua estrutura é monitorada de forma preventiva, as atualizações são feitas de forma programada e seu ambiente se torna mais produtivo e seguro.

Ficou interessado nas vantagens para sua PME? Aproveite para conhecer melhor nossos Serviços Gerenciados, converse com nosso departamento comercial ou solicite uma demonstração.

gtsolucoes.com.br
comercial@gtsolucoes.com.br
47 99189-4100

GT
Soluções em TI