ALERTA
SECURITY

5 DICAS DE CIBERSEGURANÇA QUE PODEM SALVAR O SEU NEGÓCIO

ALERTA SECURITY

Parceiros Tecnológicos:

SONICWALL · FORTIFYDATA · ZABBIX · SOPHOS · ManageEngine · HACK3R RANGERS · tenable network security · kaspersky · CLOUDFLARE · CROWDSTRIKE

ÍNDICE

INVASORES TRABALHAM 24/7

SEM APOIO PROFISSIONAL, É PRATICAMENTE IMPOSSÍVEL CONTER OS ATAQUES

Todos os dias somos testemunhas de ataques cibernéticos sofridos por empresas de diferentes portes. Geralmente, os casos das grandes marcas ganham mais notoriedade por envolverem a vulnerabilidade de sistemas sofisticados de segurança.

Segundo dados apresentados pela CrowdStrike, os últimos anos têm sido um alerta: **não existe segmento** ou país seguro. Por exemplo, **60% das pequenas e médias empresas sofreram pelo menos um ataque cibernético**, tornando-se vítimas comuns de incidentes desse tipo.

Os principais golpes implicam no **roubo de senhas corporativas, ataques via internet e na invasão da rede que explora o trabalho remoto.**

Antes uma opção, a cibersegurança se tornou um caminho crítico para as empresas evitarem prejuízos milionários.

A sua empresa está preparada para esta dura realidade?

ASSISTA AO VÍDEO E CONHEÇA A ALERTA SECURITY

O BRASIL É VÍTIMA DE MAIS DE 1.300 ATAQUES CIBERNÉTICOS *POR MINUTO

UMA HORA ELAS VÃO BATER NA SUA PORTA OU, SIMPLESMENTE, ENTRAR SEM PERMISSÃO

*Fonte: Panorama de Ameaças para América Latina 2024

Até pouco tempo atrás, produzir mais, vender mais e conquistar novos clientes era o ciclo normal de qualquer negócio de pequeno e médio porte. No entanto, isso está ameaçado por questões de segurança digital.

Sim, aquele faturamento conquistado com muito sacrifício para melhorar o fluxo de caixa, realizar investimentos e gerar novos produtos e serviços está bem perto de ser subtraído do negócio. Opções não faltam. Confira algumas delas:

Port Scanning Attack - malware que aproveita uma vulnerabilidade no sistema para fazer uma busca no servidor, visando uma brecha de segurança. Uma vez que ele encontra, rouba informações e dados com o objetivo de danificar o sistema ou sequestrar os dados.

Ransomware - bloqueia o acesso a todos os arquivos do servidor atacado. Os hackers só liberam novamente o acesso após o pagamento do valor de resgate, normalmente cobrado em bitcoins, determinado pelo sequestrador.

Cavalo de Tróia - malware popular que só funciona com "autorização" do usuário. Basta que a pessoa execute algum anexo de e-mail de remetente suspeito ou desconhecido, ou então, faça um download suspeito, contendo o vírus camuflado, e pronto: o Cavalo de Tróia está instalado. Com isso, os hackers podem roubar informações pessoais e interromper funções no computador.

Phishing - ataque cibernético no qual os hackers levam os usuários a entregarem informações sigilosas, incluindo senhas, dados bancários e CPF. Via de regra, este tipo de cibercrime direciona o usuário para um site idêntico ao verdadeiro de uma agência bancária, por exemplo. Assim, nessa página falsa, que funciona como uma "isca", os hackers "pescam" os dados dos usuários. Esse é um dos ataques cibernéticos mais populares.

Zero Day - ciberataque que busca falhas de segurança em programas ou aplicativos recém-lançados, explorando brechas e bugs antes da correção. É um ataque menos comum, mas os desenvolvedores costumam se deparar com esse tipo de ameaça cibernética.

POR QUE AS EMPRESAS BRASILEIRAS SEGUEM APAGANDO INCÊNDIO QUANDO O ASSUNTO É CIBERSEGURANÇA?

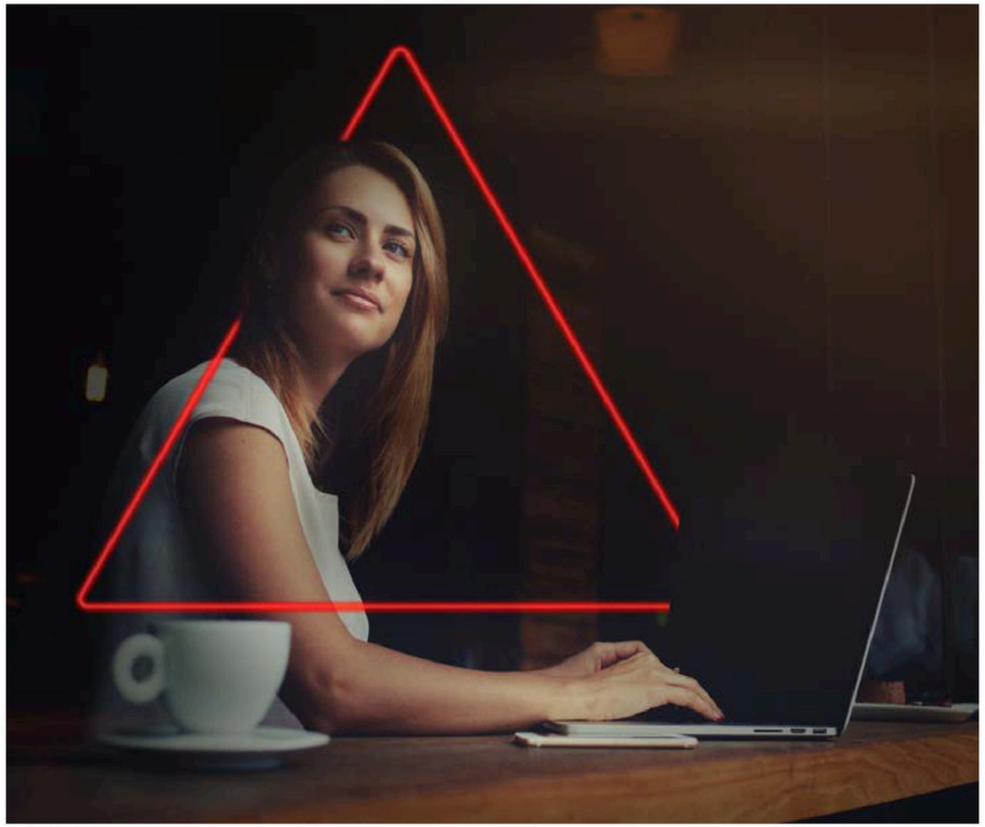
O FATURAMENTO TEM DESTINO CERTO PARA ALGUNS NEGÓCIOS E, POR VEZES, A SEGURANÇA DIGITAL NÃO É PRIORIZADA NO ORÇAMENTO

Entendemos, sim, a dificuldade em priorizar um pouco do orçamento para a segurança digital. As empresas de serviços e a indústria possuem vários investimentos que exigem grande atenção por parte dos empreendedores e gestores. Afinal, em tempos difíceis, não está sobrando recursos para ninguém, não é mesmo?

Mas, por outro lado, não dá mais para viver num cenário com pouco ou nenhum nível de segurança e proteção. Seria como ter uma bela casa e não ter muros ou portões robustos, além de alarmes básicos para evitar invasões, correto?

Pensar na segurança digital do negócio é algo que tira a tranquilidade. Por isso criamos um material que traz essa reflexão buscando sempre proporcionar uma certa tranquilidade.

Vamos lá, então!



VOLTAR AO ÍNDICE

DICA 1: COMECE PELA POLÍTICA DE SEGURANÇA CIBERNÉTICA

ESTE É O BÁSICO DO BÁSICO. IMPORTANTE É TER UM OLHAR GERAL, ANTES DE PRIORIZAR

O primeiro investimento em segurança digital deve começar pela definição da política cibernética. A princípio parece complexo, mas não é.

As políticas de cibersegurança da sua empresa devem ser criadas e implementadas para proteger seus ativos e dados, e essas políticas devem ser revisadas regularmente para garantir que estejam em conformidade com os principais frameworks de segurança.

Uma boa política deve conter uma definição clara de responsabilidades, e esses são os principais itens que devem estar nas suas políticas de cibersegurança:

1. **Criptografia de dados;**
2. **Rede wi-fi segura;**
3. **Controle de acesso às redes e sistemas;**
4. **Gerenciamento de incidentes de segurança;**
5. **Treinamento de cibersegurança para funcionários.**

Segundo o Relatório Semestral de Ameaças Cibernéticas da Sonicwall 2024, no último semestre os casos de ransomware registrados tiveram um aumento de 51% só na América Latina.

VEJA EM NOSSO BLOG: ALÉM DAS MULTAS - O VALOR REAL DE ESTAR EM CONFORMIDADE COM AS NORMAS DE SEGURANÇA CIBERNÉTICA

DICA 2: TESTE SUAS VULNERABILIDADES

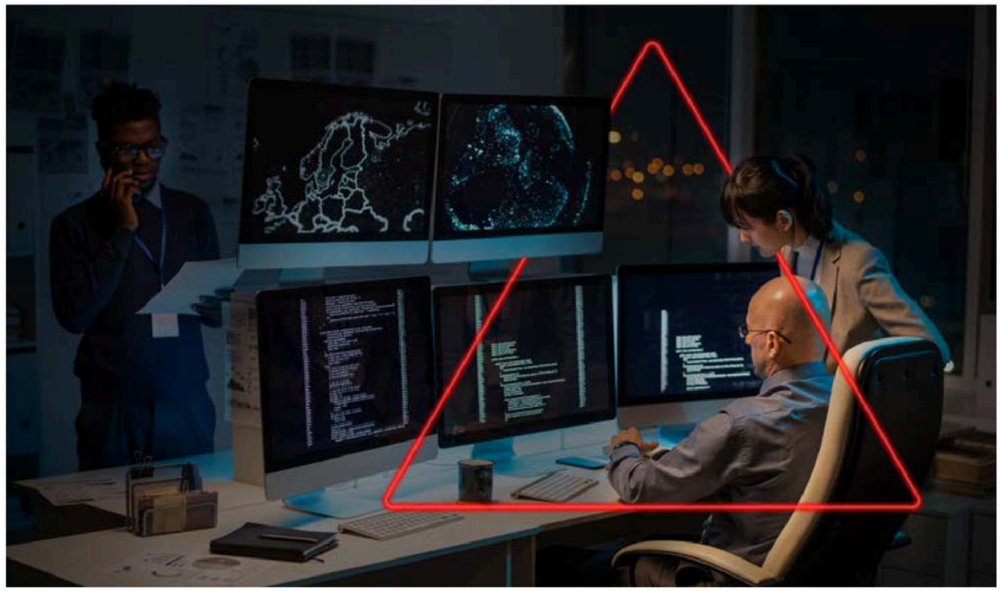
QUAL O GRAU DE VULNERABILIDADE DO SEU NEGÓCIO?

A execução de testes de vulnerabilidade e resiliência em riscos cibernéticos é um bom começo para verificar, no momento zero, quais são as fragilidades e fortalezas de sua infraestrutura. Ou seja, se existir algum problema, você já sabe como reduzir o risco no curto prazo, não é mesmo?

Em termos de segurança da informação, uma vulnerabilidade é uma fragilidade encontrada em um ativo ou em um controle e que pode ser explorada por uma ou mais ameaças, o que se torna um risco de segurança.

Uma forma de proteger as informações é através da identificação, avaliação, priorização e correção das deficiências identificadas nos ativos.

Esta atividade é conhecida como **Vulnerability Assessment** e visa encontrar as fragilidades nas plataformas de software ou hardware para resolver as falhas, antes que elas possam gerar um impacto negativo.



79% das empresas afirmam ter um plano de resposta a um possível ataque cibernético, mas apenas um terço fez algum tipo de teste preventivo. (DataFolha, 2024)

SAIBA MAIS SOBRE A SOLUÇÃO FORTIFYDATA E COMO ELA PODE TE AJUDAR NO CONTROLE DAS VULNERABILIDADES

DICA 3: CRIE UMA CONEXÃO/REDE SEGURA

ESTA INICIATIVA AUMENTA A SEGURANÇA DA SUA EMPRESA

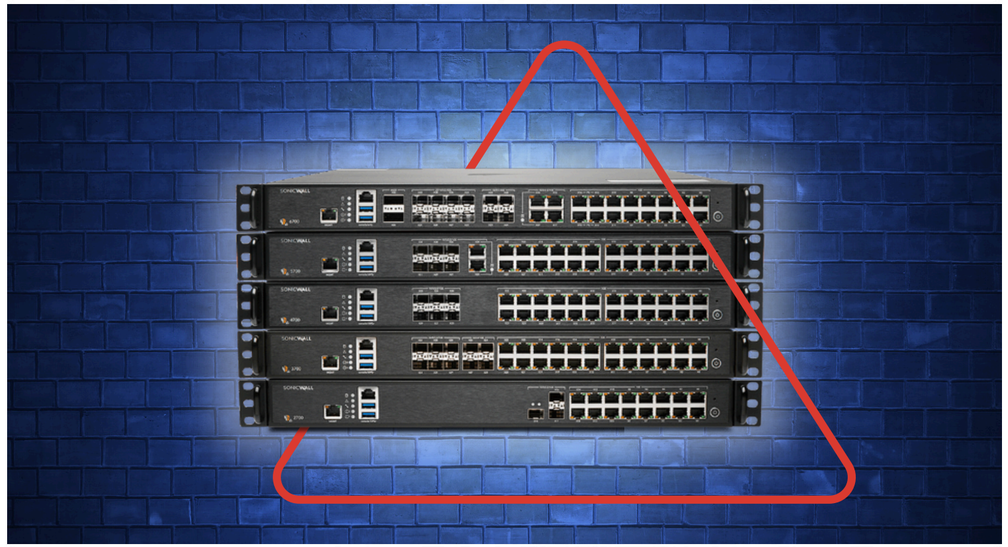
Existem alguns recursos que aumentam a segurança das informações na sua empresa e que não são complexos de serem implementados.

Um deles é adoção de uma conexão e rede seguras. Uma rede interna criada para a sua empresa. Ela pode ser criada usando Firewalls NGFW e outras ferramentas de cibersegurança.

A conexão segura é importante pois impede que pessoas não autorizadas acessem a rede de informações, além de impedir que os ataques cibernéticos sejam direcionados à sua empresa.

Para criar uma conexão/rede segura, basta:

1. **Utilizar um firewall de última geração – NGFW;**
2. **Criar usuários nominados, para navegação e acesso a rede da empresa;**
3. **Segmentar a rede da empresa.**
4. **O Firewall deve efetuar análise de pacotes criptografados. (DPI SSL)**
5. **O Firewall deve possuir feature para análise e teste de arquivos desconhecidos. (Sandbox).**
6. **Manter um software de relatórios para análise do tráfego em tempo real (visibilidade do ambiente)**



Nós queremos atuar como uma extensão da sua equipe interna de T.I. Veja como podemos fazer isso clicando aqui.

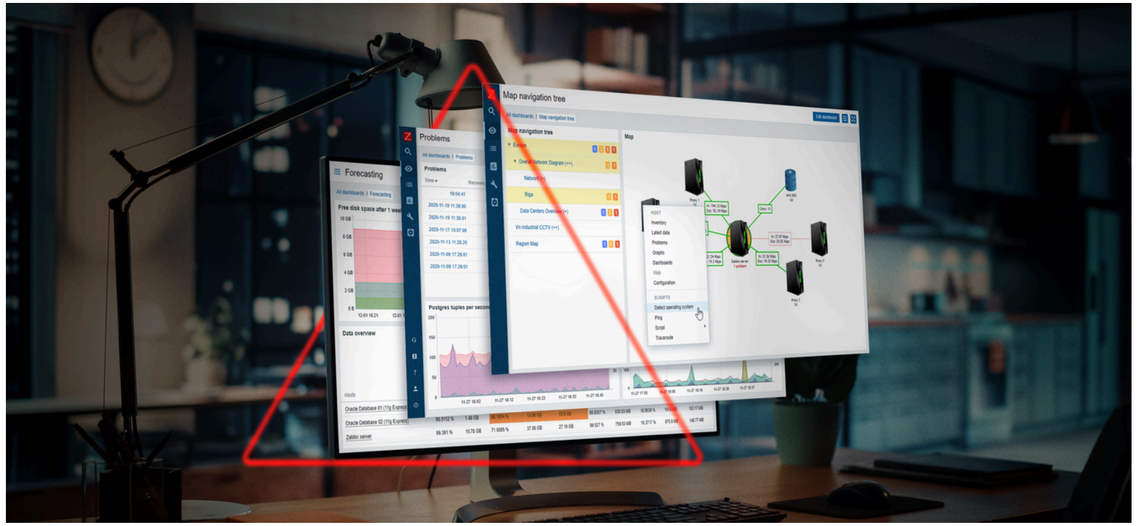
Está em dúvida sobre qual Firewall é o correto para você?

SAIBA COMO DECIDIR

DICA 4: FAÇA O INVENTÁRIO DE ATIVOS E MONITORE 24/7 SUA REDE

É IMPORTANTE A EMPRESA SABER SEUS PONTOS CRÍTICOS E MONITORÁ-LOS

A importância do monitoramento de redes: O software de monitoramento de redes tem um papel importante na sustentação dos negócios. No entanto, muitas empresas buscam essa solução apenas após o incidente. Quando usada corretamente, ela permite: **(1) Manter a disponibilidade; (2) Manter a performance; (3) Coletar dados para auxiliar na tomada de decisões.**



Quando a rede é monitorada, os responsáveis pelos processos de T.I. são informados, rapidamente, sobre possíveis falhas, fazendo com que a equipe esteja sempre atenta ao desempenho da rede, atuando de forma ágil, mesmo remotamente.

Contar com o suporte de uma equipe especializada de NSOCs (Network Security Operations Centers), proporciona **grandes benefícios**.

> Apenas 52% das empresas brasileiras adotaram algum software para monitorar, detectar e prevenir incidentes de segurança (Pesquisa online da Pollfish Inc.).

Está em dúvida sobre qual solução de monitoramento é a correta para você?

- A solução ZABBIX ARGOS faz o monitoramento contínuo e proativo para antecipar e solucionar problemas antes que estes causem danos ou paradas na operação;
- A solução de monitoramento bem implantada reduz custos de TI e infraestrutura.

SAIBA COMO DECIDIR

DICA 5: CONSCIENTIZE SUA EQUIPE DE COLABORADORES

A SEGURANÇA FAZ PARTE DE UMA NOVA CULTURA NA EMPRESA

É preciso conscientizar cada colaborador sobre os riscos e as formas de proteção. Cada departamento deve receber um tipo de treinamento, alinhado com o nível de responsabilidade e conhecimento. A equipe também precisa ser incentivada a relatar incidentes e até mesmo suspeitas.

Pensando nisso, a Alerta Security está trazendo para os seus clientes a plataforma **Hacker Rangers**, que visa promover a cultura de cibersegurança corporativa através da ***gamificação***, abordando temas relacionados à segurança de dados tanto no ambiente da empresa quanto em home office.

A solução apresenta a nova legislação e suas exigências de forma simples e clara, apoiada por exemplos e situações comuns à rotina de trabalho dos colaboradores, usando vídeos, textos e questionários em um ambiente online descontraído.

A Plataforma Hacker Rangers conta com mais de **400 minicursos, atendendo mais de 300 empresas**, que já aprenderam a adotar hábitos seguros de proteção de dados.

Você sabia? Mais de 80% dos ataques/incidentes de segurança são originados por falha humana dos usuários e colaboradores internos. (Leia a matéria completa em nosso blog clicando aqui)

TESTE GRÁTIS A SOLUÇÃO HACKER RANGERS POR 15 DIAS

NÓS ESTAMOS PREPARADOS PARA PROTEGER O SEU NEGÓCIO


Proteção de dados


Monitoramento de T.I.


Acesso Remoto Seguro


Estratégia em Defesa Cibernética

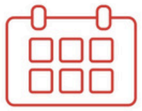
Centro de Operações NSOC

Conclusão

Os gestores de TI concluíram que o custo mensal para manter uma equipe interna de Analistas de TI com alguma especialização em Segurança da Informação é muito alto. Além da necessidade de investimentos continuados em treinamentos, capacitação, certificação de fabricantes e altos salários, os colaboradores precisam executar várias tarefas tediosas ao mesmo tempo, e a empresa precisa lidar com o risco de mudanças e os custos da rotatividade de pessoal.

No centro disso tudo, um bom fornecedor pode unificar e facilitar todas estas rotinas remotamente, contribuindo para aumentar significativamente o nível de segurança do seu ambiente corporativo.

AGENDE UM DIAGNÓSTICO GRATUITO


+ de 20 anos de mercado
Desde 2004


Colaboradores treinados e certificados


+ de 150 clientes gerenciados
Via S-NOC 24/7 próprio


+ de 1800 projetos
Implantados


Escritórios em São Paulo
Santa Catarina e Orlando/EUA

Nota 10 em atendimento

Após a pesquisa de Net Promoter Score (NPS), o atendimento da Alerta obteve nota máxima e comprovou sua excelência e comprometimento (leia mais).

A Alerta Security Solutions é um provedor de serviços gerenciados de segurança e monitoramento remoto, atuando no modelo Managed Security Services - MSS, que vai além da venda de ferramentas operacionais ou dispositivos de segurança pontuais. Nossas soluções são oferecidas 100% em formato de assinatura mensal no modelo SaaS.

VEJA O QUE DIZEM NOSSOS CLIENTES:

"A implementação das soluções de Firewall de última geração (NGFW) aumentou significativamente a segurança do ambiente corporativo. Nossa empresa se sente muito confortável com o suporte continuado 24/7 fornecido pela ALERTA SECURITY, temos apoio com orientação profissional para planejamento de novas tecnologias e novos projetos."

Christian Mineff
Gerente de Infraestrutura de TI – UNIVERSIDADE BRASIL
Cliente desde 2014

"À medida que expandimos nossas filiais remotas, administrar as rotinas do ambiente de Firewall estava se tornando mais trabalhoso. A nossa equipe interna de TI precisava contar com apoio de especialistas 24/7 próximos e ágeis para fornecer Suporte Mensal, acompanhamento e análise de atividades suspeitas."

José Ricardo Garcia
Coordenador de TI - TBFORTE
Cliente desde 2010

"Nossa empresa se sente muito confortável com a ALERTA SECURITY. Do suporte remoto especializado 24/7 com enfoque na Segurança da Informação ao apoio no planejamento de novas tecnologias e novos projetos, estamos tomando decisões mais seguras e com orientação profissional."

Jonatas Gaudência
Coordenador de TI - NOVAQUEST
Cliente desde 2013

"A aquisição e implementação das soluções de Firewall de última geração (NGFW) melhorou significativamente a segurança do ambiente corporativo. A ALERTA SECURITY tem contribuído de forma efetiva e muito profissional no planejamento de novas tecnologias e novos projetos na área de segurança da informação."

Rodrigo Monteiro
Gerente de TI – SETIS AUTOMAÇÃO
Cliente desde 2011

ALERTA
SECURITY

EXCELÊNCIA NPS 10 EM ATENDIMENTO

MAIS DE 20 ANOS ATUANDO EM DEFESA CIBERNÉTICA

+55 11 3105-8655

CONTATO@ALERTASECURITY.COM.BR

RUA PAIS LEME, 215 - 14º ANDAR - PINHEIROS, SÃO PAULO - SP