ALERTA
SECURITY

SONICWALL™

5 DICAS DE CIBERSEGURANÇA QUE PODEM SALVAR O SEU NEGÓCIO

ALERTA
SECURITY

Parceiros tecnológicos

SONICWALL ZABBIX FORTIFYDATA tenable kaspersky LUMU HACK3R_RANGERS

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 relatório da SonicWall, o ano de 2022 foi um alerta: **não existe segmento** ou país seguro. Os **pequenos e médios negócios**, por exemplo, se tornaram vítimas comuns, registrando um **aumento de 41% dos ataques cibernéticos** no primeiro semestre de 2022 em relação ao mesmo período de 2021.

De acordo com a pesquisa, 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 SOFRE 1.554 TENTATIVAS DE ATAQUES DE MALWARE POR MINUTO*

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

Kaspersky, 2022.

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 DO SETOR DE SERVIÇOS E DA INDÚSTRIA NÃO PRIORIZAM ESTE ASSUNTO?

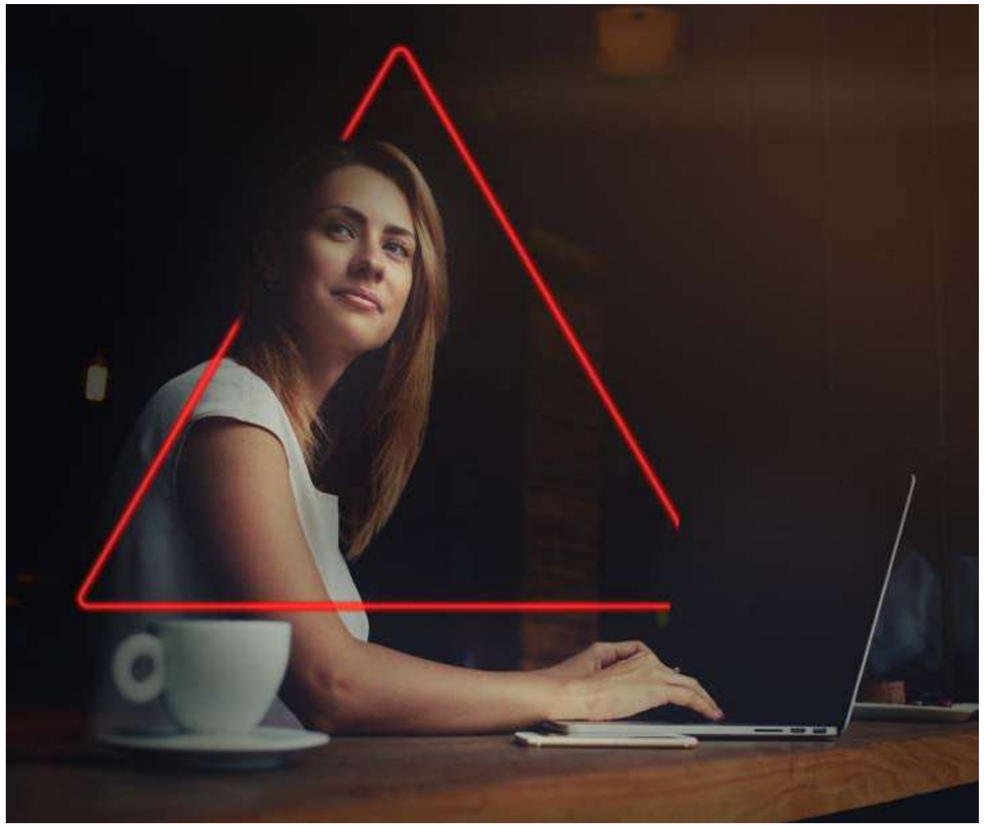
O FATURAMENTO TEM DESTINO CERTO PARA ALGUNS NEGÓCIOS E, POR VEZES, A SEGURANÇA DIGITAL NÃO É PRIORIZADA NO ORÇAMENTO

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 PELAS POLÍTICAS 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 os seus ativos e dados, e essas políticas devem ser revisadas regularmente para garantir que estejam sempre atualizadas.

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.**

O Brasil aparece entre os 10 países com maior número de ataques de ransomware em 2021. Aproximadamente 61% dos ataques são das famílias: Ryuk, SamSam e Cerber (2022 SonicWall Cyber Threat Report).

AGENDE UM DIAGNÓSTICO GRATUITO

DICA 2: TESTE SUAS VULNERABILIDADES

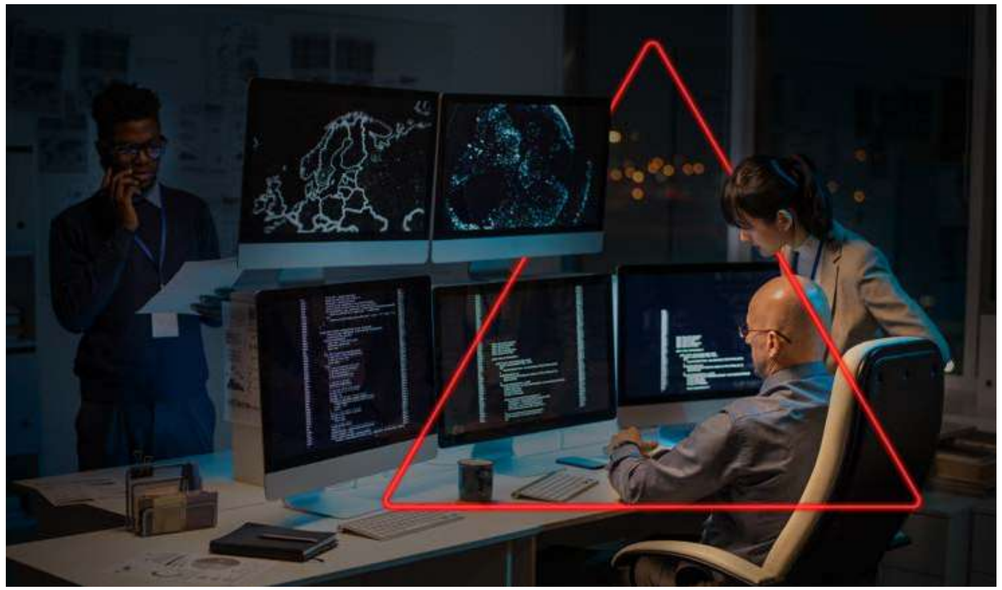
VALE VERIFICAR O QUE ESTÁ SEGURO OU NÃO

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.



83% das empresas testam seus ativos críticos apenas uma vez por ano (The ROI of Modern Pentesting Report, 2021).

FAÇA UMA DEGUSTAÇÃO TÉCNICA GRATUITA DO SEU IP DE WAN

DICA 3: CRIE UMA CONEXÃO ISOLADA OU INTRANET

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 a conexão isolada ou intranet. Uma rede interna criada para a sua empresa. Ela pode ser criada usando firewalls e outras ferramentas de cibersegurança.

A conexão isolada 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 isolada, 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)

Malwares enviados por HTML aumentaram 167% (2022 SonicWall Cyber Threat Report).

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

Praticamente toda semana nos damos conta de que alguma nova tecnologia, pessoa ou recurso passou a fazer parte da empresa. Passado poucos meses, é impossível ter a exata noção do que é novo e antigo, certo?

É por isso que as empresas devem identificar seus ativos e classificar as informações críticas.

O monitoramento dos sistemas e redes da sua empresa é importante para **detectar problemas de cibersegurança em tempo real**, o que permite a tomada de medidas para corrigir o problema antes que ele cause danos à sua empresa.

Além disso, o **monitoramento** também pode ajudar você a identificar tendências de riscos em cibersegurança que podem afetar sua empresa no futuro.

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: TREINE SUA EQUIPE DE COLABORADORES

A SEGURANÇA FAZ PARTE DE UMA NOVA CULTURA NA EMPRESA

Com o grande volume de tecnologias e prevenção a ataques, é comum que os profissionais fiquem confusos ou despreparados para lidar com tanta informação.

As equipes de TI são responsáveis por garantir que os sistemas e redes da sua empresa estejam seguros. É importante treiná-las para que elas saibam como lidar com problemas de cibersegurança.

Além do treinamento, é necessário que essas equipes sejam testadas regularmente, para garantir que estejam preparadas para lidar com problemas e vulnerabilidades.

Vale lembrar que a cibersegurança é um processo contínuo e que ameaças cibernéticas estão sempre evoluindo. Portanto, é essencial manter-se atualizado com as últimas tendências e fazer ajustes na sua política de segurança quando necessário.

24,3% dos colaboradores ignoram a ameaça porque não sabem como resolvê-la (Estudo Breakthrough - Divulgado pelo Crypto ID).

AGENDE UM DIAGNÓSTICO GRATUITO

ESTÁ NA DÚVIDA SE SUA EMPRESA PRECISA DE UM PARCEIRO ESPECIALIZADO EM CIBERSEGURANÇA?

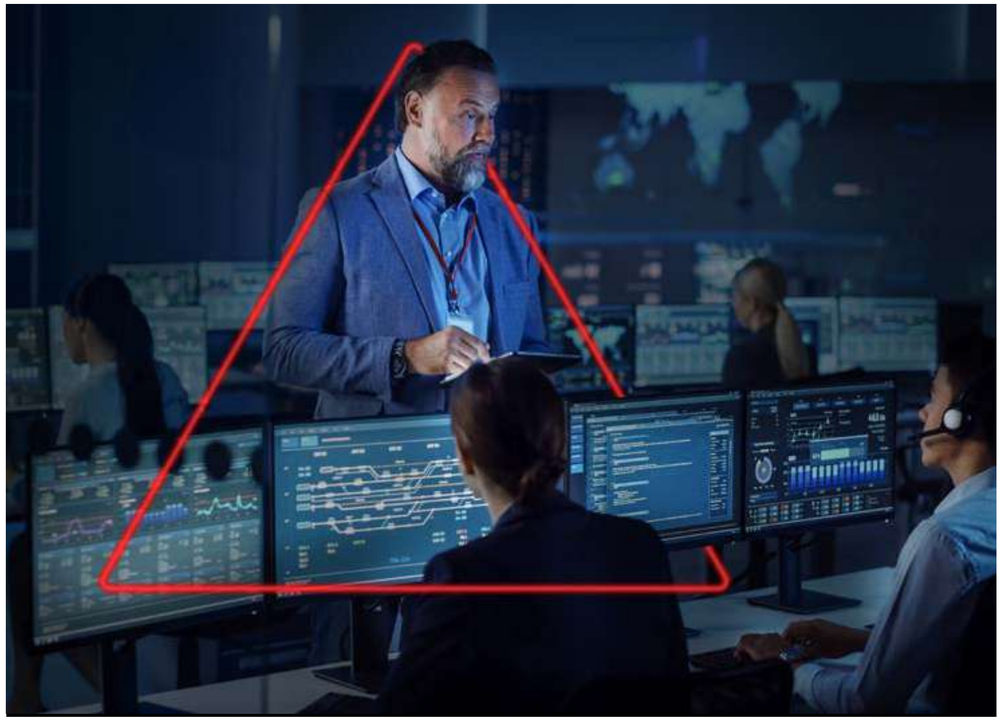
1. Como a liderança executiva da sua empresa se mantém atualizada sobre o nível e o grau de impacto dos riscos de cibersegurança para a empresa?

2. Quais são os planos ou estratégias de segurança de dados para lidar com os riscos que foram identificados?

3. Como, especificamente, seu programa atual de segurança de dados aplica os padrões da indústria e as melhores práticas?

4. Quantos e quais tipos de incidentes de cibersegurança são detectados na empresa toda semana? E qual o grau de risco que dispara um alerta direto para a liderança executiva?

5. Seu plano de resposta a incidentes de cibersegurança é rígido? Quantas vezes por semana ou por mês ele é testado?



Se você não tem resposta para qualquer uma das 5 perguntas acima, nós podemos melhorar significativamente o nível de segurança da sua empresa.

ASSISTA AO VÍDEO E CONHEÇA A ALERTA SECURITY

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

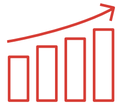
Os gestores de TI concluíram que o custo mensal para manter uma equipe interna de Analistas de TI com alguma especialização em Segurança da Informação é muito alto. Além da necessidade de investimentos continuados em treinamentos, capacitação, certificação de fabricantes e altos salários, os colaboradores 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.

+ de 18 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

A Alerta Security Solutions é um provedor de serviços gerenciados de segurança e monitoramento remoto. Atualmente possuímos uma carteira com mais de 150 empresas gerenciadas em regime 24x7x365. Atuamos 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.

AGENDE UM DIAGNÓSTICO GRATUITO

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

MAIS DE 18 ANOS ATUANDO EM DEFESA CIBERNÉTICA

+55 11 3105-8655

CONTATO@ALERTASECURITY.COM.BR

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

CONHEÇA A ALERTA SECURITY