AUTO ASSESSMENT de cibersegurança EM 10 PASSOS

Sem dúvida, priorizar a segurança da informação é um acerto muito grande. Inclusive, pesquisas recentes mostram que

MAIS DE 90% DOS ATAQUES DE VIOLAÇÃO DE DADOS REGISTRADOS NOS ÚLTIMOS ANOS PODERIAM SER EVITADOS.

Ou seja, o levantamento comprova que as ameaças cibernéticas são muitas vezes ignoradas, ou passam despercebidas pelas empresas. Dessa forma, você já deve imaginar a importância de diagnosticar os riscos do seu negócio.

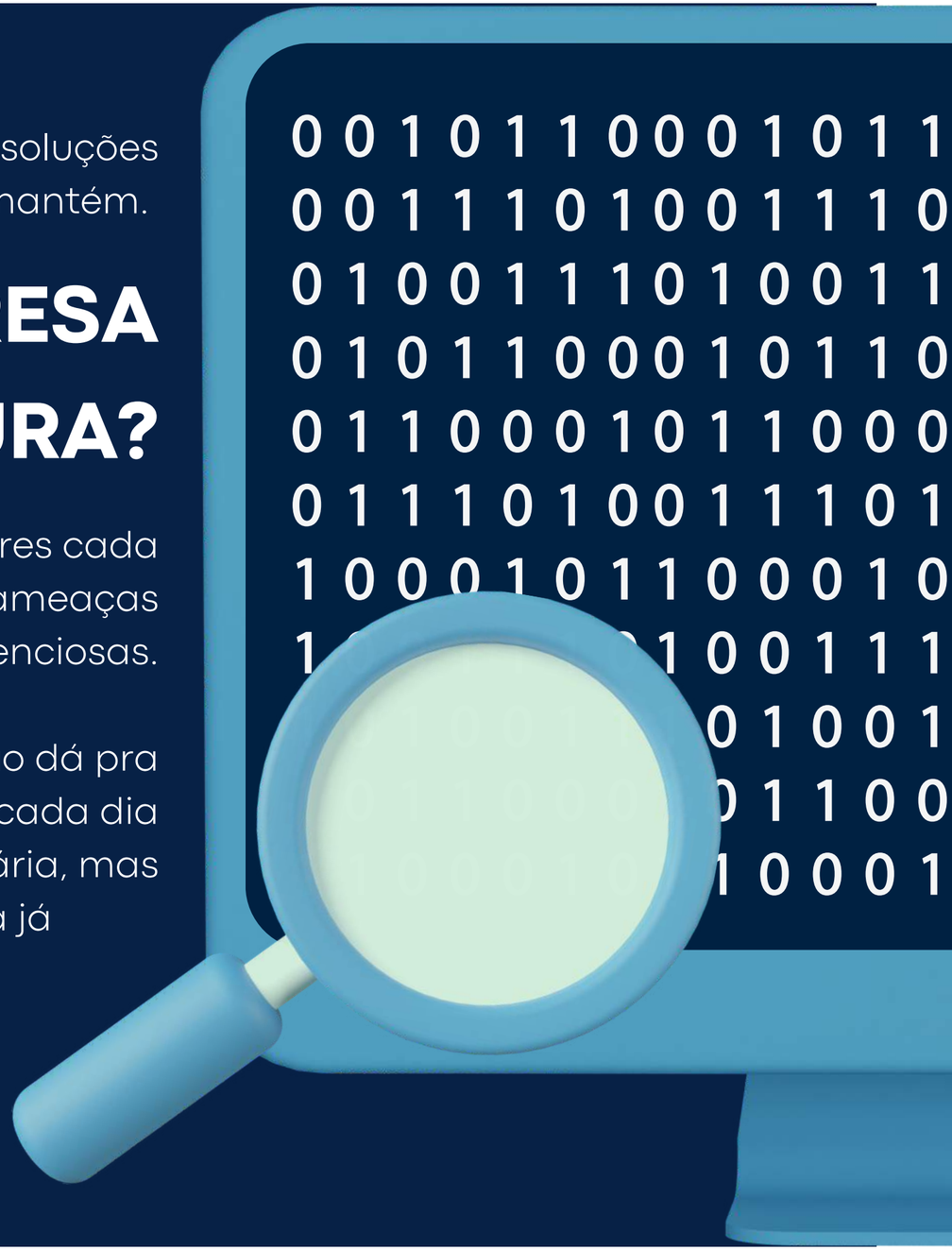
NEXT4SEC SECURITY INTELLIGENCE

Além disso, mesmo se sua empresa já contar com diversas soluções de segurança implantadas, uma dúvida sempre se mantém.

SERÁ QUE MINHA EMPRESA ESTÁ MESMO SEGURA?

Leis de segurança de dados, falta de conscientização, malwares cada vez mais inteligentes, erros humanos diários e diversas outras ameaças que, muitas vezes, podem ser completamente silenciosas.

Nesse cenário, mesmo com as mais avançadas soluções, não dá pra deixar os pés pro alto. A segurança vem e continuará sendo cada dia mais complexa, não apenas como um serviço ou ação temporária, mas como um processo contínuo. Por isso, mesmo que sua empresa já priorize a cibersegurança, sempre vale mais uma avaliação.



NEXT4SEC SECURITY INTELLIGENCE

O assessment de segurança permite que você conheça o cenário atual do seu ambiente de TI e identifique os pontos que expõem seus dados e sua empresa a ataques, invasões, sequestro e perda de dados. Nesse e-book, você descobrirá como fazê-lo em apenas 10 passos.

Lembramos que o autoassessment realizado internamente, por mais completo que seja, não substitui uma avaliação profissional feita por um especialista na área de cibersegurança.

Antes de qualquer coisa, é necessário ter conhecimento sobre a base do seu ambiente: os ativos. Servidores, informações de contato dos clientes, documentos críticos, segredos comerciais e outros itens são exemplos de alguns. Contando com a ajuda de todos os departamentos da empresa, deve-se fazer uma lista abrangente de todos os ativos para saber o que precisa ser protegido.

1

Se você já tem uma boa visibilidade dos ativos da sua rede e de sua criticidade, bem, já começamos a avaliação de risco.

2 IDENTIFIQUE AS AMEAÇAS

Uma ameaça pode ser qualquer acontecimento que cause danos aos ativos ou processos corporativos. As ameaças podem ser internas ou externas, bem como maliciosas ou acidentais; como por exemplo desastres naturais, falha de sistemas, interferência humana etc. É, então, essencial realizar uma triagem completa para todas as ameaças em potencial.

4 ENCONTRE AS VULNERABILIDADES

Uma vulnerabilidade é uma fraqueza que pode ser explorada por cibercriminosos para obter acesso não autorizado a um sistema. As vulnerabilidades podem ser físicas (como equipamentos antigos), problemas de software ou configuração (como permissões de acesso excessivos ou estação de trabalho não atualizadas), ou fatores humanos (como membros da equipe descuidados ou não treinados).

Análise, relatórios de auditoria, métodos de teste e avaliação de segurança da informação (ST&E), podem ser usados para identificar vulnerabilidades. Entretanto, não se deve esquecer das falhas humanas. Para estas, é necessário analisar qual o nível de conscientização e preparo dos colaboradores em práticas simples de cibersegurança.

3 AVALIAÇÃO DE CONTROLES

Políticas de segurança, medidas administrativas e processos físicos e ambientais são exemplos de controles não técnicos que devem ser revisados nessa fase do assessment. A organização deve trabalhar em políticas, procedimentos e sensibilização dos colaboradores, clientes e parceiros, provendo normas e treinamentos com relação ao uso de ativos.

NEXT4SEC SECURITY INTELLIGENCE

5

PRIORIZAÇÃO

A gravidade de cada ameaça é determinada de acordo com sua probabilidade de ocorrência e seu impacto. O cálculo do valor fornecerá uma escala de priorização de risco, que permitirá que as equipes de segurança se concentrem naqueles com maior gravidade.

6

AVALIAÇÃO DE RISCO

O risco diz a respeito do potencial da ameaça de explorar as vulnerabilidades do ambiente e causar prejuízo em um ou mais ativos, resultando em perda monetária. Avalie o risco de acordo como descrito acima e defina cada um em alto, moderado ou baixo. Então, desenvolva uma solução para cada risco de nível moderado ou alto;

NEXT4SEC SECURITY INTELLIGENCE

AMEAÇA	VULNERABILIDADE	ATIVOS E CONSEQUÊNCIA	RISCO	SOLUÇÃO
Falha no sistema Superaquecimento nos servidores **ALTO**	Sistema de ar condicionado antigo, com mais de 10 anos **ALTO**	**Servidores** Todos os serviços estarão indiponíveis por no mínimo 3 horas **CRÍTICO**	Perda potencial de R$50.000 por ocorrência **ALTO**	Compra de um ar condicionado mais moderno (custo: R$10.000)
Interferência humana maliciosa Ataque de DDoS **ALTO**	Firewall configurado de forma indevida contendo uma boa forma de mitigação **BAIXO**	**Website** O website estará indisponível. **CRÍTICO**	Perda potencial de R$20.000 por hora a cada ocorrência **MODERADO**	Monitormento avançado do firewall
Desastre natural Enchente **MODERADO**	Sala de servidores está no terceiro andar **BAIXO**	**Servidores** Todos os servidores estarão indisponíveis **CRÍTICO**	**BAIXO**	Sem ação necessária
Interferência humana acidental Exclusão acidental de arquivos **ALTO**	Permissões estão configuradas corretamente, com softwares de auditoria e backups. **BAIXO**	**Todos os arquivos em um FIle Share** Dados críticos podem ser perdidos, mas poderão ser recuperados **MODERADO**	**BAIXO**	Continuar o monitoramento de acessos e usuários privilegiados e backups.

NEXT4SEC SECURITY INTELLIGENCE

7 CRIE UM PLANO DE GERENCIAMENTO DE RISCO

Com os dados coletados nas outras fases do assessment, crie um esquema que reúna todas as possíveis ameaças, seu nível de risco, consequências para o negócio e possíveis soluções. Assim, é possível ter uma fácil visualização dos riscos de toda a rede.

A equação básica envolve apenas três fatores: a importância dos ativos em risco, o quão crítico a ameaça é e quão vulnerável está o sistema a essa ameaça.

8 ELABORE UMA ESTRATÉGIA

Crie uma estratégia que aprimore a infraestrutura de TI para mitigar as ameaças e vulnerabilidades observadas como mais críticas nos passos anteriores. Estude quais medidas devem ser tomadas a curto e longo prazo, o que pode ser resolvido internamente e o que buscar ajuda externa.

9 RELATÓRIO DE AVALIAÇÃO

Por fim, deve-se criar um relatório que indique o objetivo da avaliação, detalhe todas as questões avaliadas no processo e proponha as melhorias necessárias diante dos resultados da avaliação.

NEXT4SEC SECURITY INTELLIGENCE

10

BUSQUE UMA PARCERIA DE CIBERSEGURANÇA PARA TE ACOMPANHAR NA MISSÃO DE TORNAR A SUA EMPRESA MAIS SEGURA

Apesar dos primeiros passos virem internamente, o essencial é contar com um parceiro de TI que possa auxiliá-los, contando com expertise e experiência no mercado.

O autoassessment não deve e nem irá substituir um assessment profissional. Mas, a boa notícia é que você pode realizar um assessment com profissionais de cibersegurança gratuitamente agora mesmo.

SOLICITE UM ASSESSMENT

OU FALE COM UM CONSULTOR **AQUI**

NEXT4SEC SECURITY INTELLIGENCE

NEXT4SEC
SECURITY INTELLIGENCE

Sobre a Next4Sec

Ciberameaças crescem de forma avançada e estratégica a cada dia, resultando em grandes riscos para negócios. Na Next4Sec, garantimos a proteção da sua empresa para que sua equipe e tenha foco total na produtividade, enquanto cuidamos da sua segurança pra você.

Com mais de 10 anos de expêriencia, somos uma empresa de Consultoria em Cibersegurança e gestão de TI. Nossas soluções abrangem gestão de segurança da informação, gestão de vulnerabilidade, suporte especializado de T.I. e programas conscientização de segurança.

Usamos nossa vasta experiência na indústria para desenvolver soluções inovadoras para os seus desafios de TI que vão poupar seu tempo, dinheiro, stress e, que acima de tudo, vão permitir que você continue com o foco no seu negócio.