"SEGURANÇA DE PONTA A PONTA:

O QUE TODO CIO PRECISA SABER"

2S
Transforme sua empresa com tecnologia

cisco
Gold Partner

ÍNDICE

Todo projeto é de Segurança da Informação

Por Renato Carneiro

Do lançamento dos smartphones e popularização da banda larga até o surgimento dos servidores de cloud computing e sistemas de virtualização, muita coisa mudou na forma de acessar e processar informações. As companhias estão cada vez mais tecnológicas e digitalizadas, com dados sendo armazenados em diferentes lugares e acessados por diversos dispositivos. As ameaças à segurança da informação acompanharam esse movimento, ganhando cada vez mais complexidade. Como consequência, a área de tecnologia da informação das empresas teve de dar uma resposta à altura. Hoje, é impossível dissociar investimento em TI do investimento em segurança da informação.

Apesar de tanto se falar sobre a importância da proteção de dados, ainda vemos muitas companhias vulneráveis. Segundo o relatório anual de segurança da Cisco, dos 115 mil dispositivos analisados, 106 mil tinham vulnerabilidades conhecidas no software, o que representa 92% no total. Em muitos deles, a versão do software em execução estava desatualizada em sua infraestrutura de rede e continha, em média, 26 vulnerabilidades. Isso quer dizer que os dispositivos não estavam nem recebendo correções para brechas conhecidas, nem informações sobre novas ameaças. Como bem diz Cezar Taurion, especialista em TI e CEO da Litteris Consulting, a cada dia surge uma novidade sobre ataques cibernéticos - e alguns podem acabar com uma empresa inteira. “À medida que a sociedade se automatiza, tudo fica mais frágil e a segurança é fundamental. Se os sistemas de comunicação, financeiro e de transporte forem invadidos, um país inteiro pode parar”, diz.

“O ideal é que todos os projetos possuam uma camada de inteligência, tendo a segurança como um habilitador”, nos contou Fabio Peake, gerente de desenvolvimento de segurança da Cisco. Neste e-book, você vai entender melhor o cenário de ameaças atuais e como se preparar. Porque todo projeto de TI - seja de colaboração, data center, mobilidade ou qualquer outro - é, também, de segurança da informação. E quem não estiver preparado deve saber: está vulnerável.

2. O RISCO DO ULTRAPASSADO

À medida que as organizações se tornam mais digitais, seu crescimento depende da capacidade de proteger toda a plataforma para que os profissionais possam trabalhar com segurança e com o acesso a todas as informações. Porém, na contramão dessa evolução, a maioria das empresas ainda conta com infraestruturas de rede antigas e ultrapassadas - principal problema para a segurança da informação, como aponta o relatório anual de segurança da Cisco. Segundo o estudo, 92% dos dispositivos analisados rodam softwares com vulnerabilidades conhecidas, 31% estão fora de linha e 8% no fim da vida (veja mais dados no gráfico da página 5). É importante a conscientização de que, por mais que a tecnologia esteja funcionando depois de três ou quatro anos de uso, não está atualizada para a proteção de novas ameaças – que evoluem com a mesma rapidez que a tecnologia. "O fabricante não investe em pesquisas e desenvolvimento para corrigir possíveis falhas ou inovar uma tecnologia antiga. O foco sempre está na criação de novas soluções", diz Fabio Peake, gerente de desenvolvimento de segurança da Cisco. Segundo ele, as ferramentas, hoje, mesclam a segurança com a infraestrutura, agindo como um habilitador, o que não acontece com as antigas.

O cenário é reflexo de uma TI pouco valorizada e estratégica, na qual a responsabilidade do bom andamento e segurança dos sistemas estava apenas nas mãos do CIO e de um técnico, que atuava sozinho. "A segurança sempre foi considerada a última prioridade das empresas. O problema precisava surgir para se tomar uma providência, o que ainda acontece em muitas companhias - aquele pensamento retrógrado de que, se está funcionando, pode ficar como está", explica Cezar Taurion, especialista em TI e CEO da Litteris Consulting. Segundo ele, o Brasil precisa evoluir muito para alcançar a maturidade de mercados como o europeu e o americano, até por uma questão social. Ele cita o setor financeiro como o mais preocupado e que mais investe em segurança e, os de saúde, educação e manufatura, como os menos envolvidos no tema.

"O fabricante não investe em pesquisas e desenvolvimento para corrigir possíveis falhas ou inovar uma tecnologia antiga. O foco sempre está na criação de novas soluções"

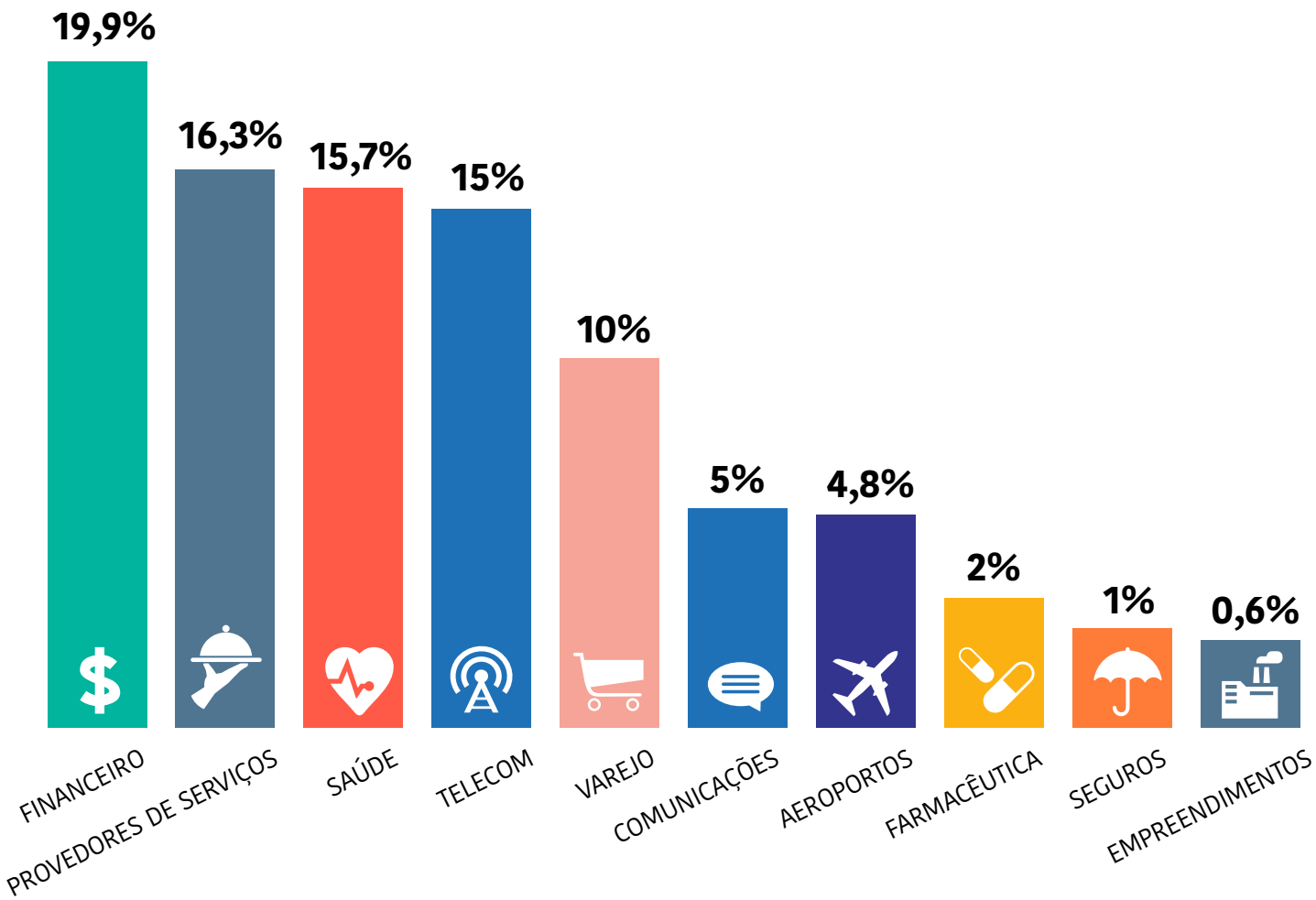
"As empresas precisam, o quanto antes, realizar patchs de correção de vulnerabilidades. Senão, estarão sujeitas à perda de dinheiro e, até, sequestro de dados vitais para o negócio", diz Taurion, ressaltando que resolver um problema é sempre mais caro do que impedir que ele aconteça.

TEMPO DE USO

Um ponto crítico, segundo a pesquisa, é a falta de entendimento sobre o tempo de uso dos dispositivos de infraestrutura (que varia de acordo com o setor). Os devices analisados já haviam atingindo o seu último dia de suporte (LDoS): não estavam nem recebendo correções para vulnerabilidades conhecidas, muito menos informações sobre novas ameaças. Veja a seguir mais informações:

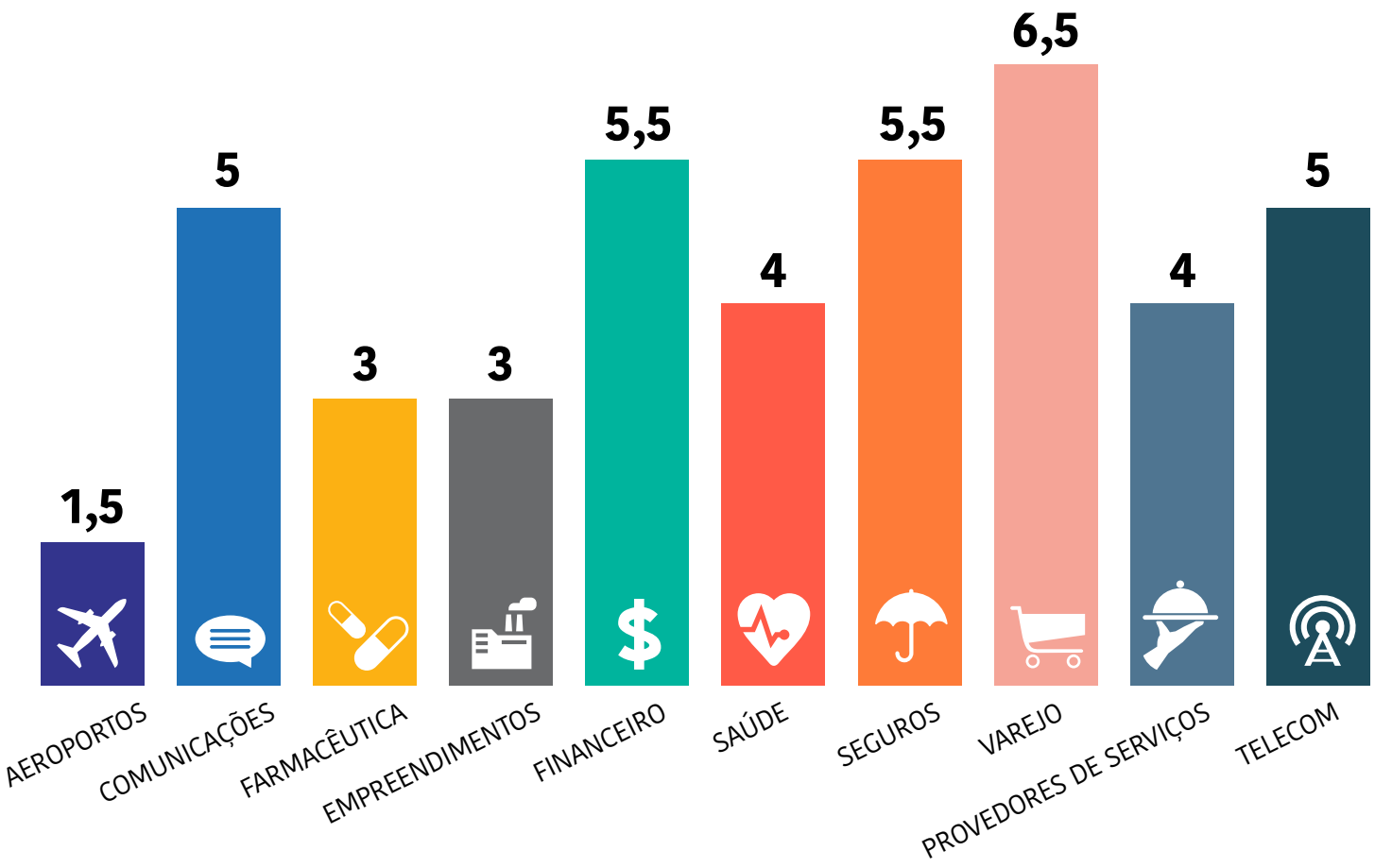
Ainda dá tempo de atualizar?

Percentual de LDoS para dispositivos de infraestrutura*



Quantos anos eles duram?

A média de idade dos softwares, por setor*



*Fonte: Relatório Anual de Segurança da Cisco, 2016.

3. DE PONTA A PONTA

Os criminosos digitais estão bem preparados tecnologicamente e, geralmente, possuem muito conhecimento sobre o nível de segurança da maioria das empresas, o que torna mais fácil a criação de técnicas inovadoras de invasão para ultrapassar as barreiras de segurança convencionais, como firewall e IPS (Sistema de Prevenção de Intrusão), que estão na borda da rede.

Os ataques evoluem rápido - o que estava em destaque em uma semana pode não ser na outra - e as empresas precisam acompanhar esse ritmo. Há poucos anos, o tema da vez eram as APTs (advanced persistent threat ou ameaça persistente e avançada); hoje fala-se em ransomware, tipo moderno de malware que sequestra o ingresso a computadores e arquivos e só o libera mediante o pagamento de um resgate extremamente caro, feito, normalmente, por meio de bitcoins. “Sem o pagamento, a empresa para. Imagine um hospital sem ter acesso aos dados de seus pacientes?”, ressalta Peake, da Cisco. Isso, além de gerar prejuízo financeiro, pode comprometer seriamente a imagem e reputação da companhia. A indústria do cibercrime, baseada em ganhos financeiros, está cada vez mais forte. “Se houver brecha, o ataque acontece”, diz.

Tais técnicas, na maioria das vezes, envolvem o usuário por ser o elo mais frágil, mas existem outras pontas que devem ser observadas para a implantação de uma estratégia de segurança eficaz. Há ameaças que, independentemente da época ou do avanço tecnológico, devem ser consideradas pelos CIOs:

1. Má conduta dos funcionários

Há duas condutas que podem incorrer no vazamento de informação: o despreparo do usuário, que utiliza senhas fáceis - quando as utiliza - e até mesmo a má conduta intencional."É bem comum os criminosos utilizarem campanhas de ataques com foco em e-mail ou via acesso web, no qual induzem as pessoas a clicar em um código malicioso ou baixar malwares para suas máquinas", explica Rodrigo dos Santos, engenheiro de sistemas da 2S. Segundo ele, a educação e conscientização dos usuários devem ter destaque na estratégia de segurança de qualquer empresa. "É necessário também proteger a máquina do usuário com visibilidade e controle dentro ou fora da rede, no caso funcionários móveis", diz. Santos recomenda que o primeiro passo seja a definição de uma política de segurança: um documento contendo o que é ou não permitido, assim como as obrigações e responsabilidades de cada um. "Quando olhamos as empresas, a maioria não tem sequer um ponto de referência para criar as políticas de controle de acesso e ter autonomia para cobrar os colaboradores em caso de desvio de conduta, já que eles não foram informados sobre o que era permitido fazer", completa.

2. Malwares que interceptam e roubam informações

De maneira simples, malware é qualquer código de software feito com a intenção de prejudicar dados, dispositivos ou pessoas, e pode se apresentar em forma de vírus, cavalos de troia (trojans) ou spyware e similares. Eles entram na rede corporativa com ajuda de e-mails, pendrives e outros dispositivos contaminados. Uma vez no ambiente, escolhem informações sensíveis e as levam para fora da infraestrutura da empresa. Cada malware tem sua própria maneira de infectar e danificar computadores e dados, por isso, requerem um método de remoção diferente. Evitar e-mails, links ou

websites suspeitos são bons hábitos online, mas não bastam. Às vezes, o ataque compromete até os websites legítimos. Entre as maneiras de se proteger ou remover uma infecção está o uso de antivírus, firewalls e segurança dos endpoints e servidores. Segundo Santos, muitas empresas preocupadas com a segurança estão utilizando, como complemento de segurança, sistemas de detecção de intrusão e malwares baseados em anomalias para melhorar a identificação de atividades mal-intencionadas por meio de perfil de tráfego, antes mesmo que se consolidem, além de backups offline para se recuperar mais rápido de incidentes.

3. Lógica x física

Quando se aborda segurança da informação, as companhias investem em proteção contra malwares e soluções de endpoint. No entanto, é importante abordar também a segurança física do ambiente. Aqui algumas perguntas são importantes: pessoas não autorizadas estão tendo acesso a ambientes restritos? Onde ficam guardados os arquivos físicos da diretoria? O que é feito com os rascunhos de reuniões estratégicas? Há câmeras de vigilância no ambiente? Há catracas?

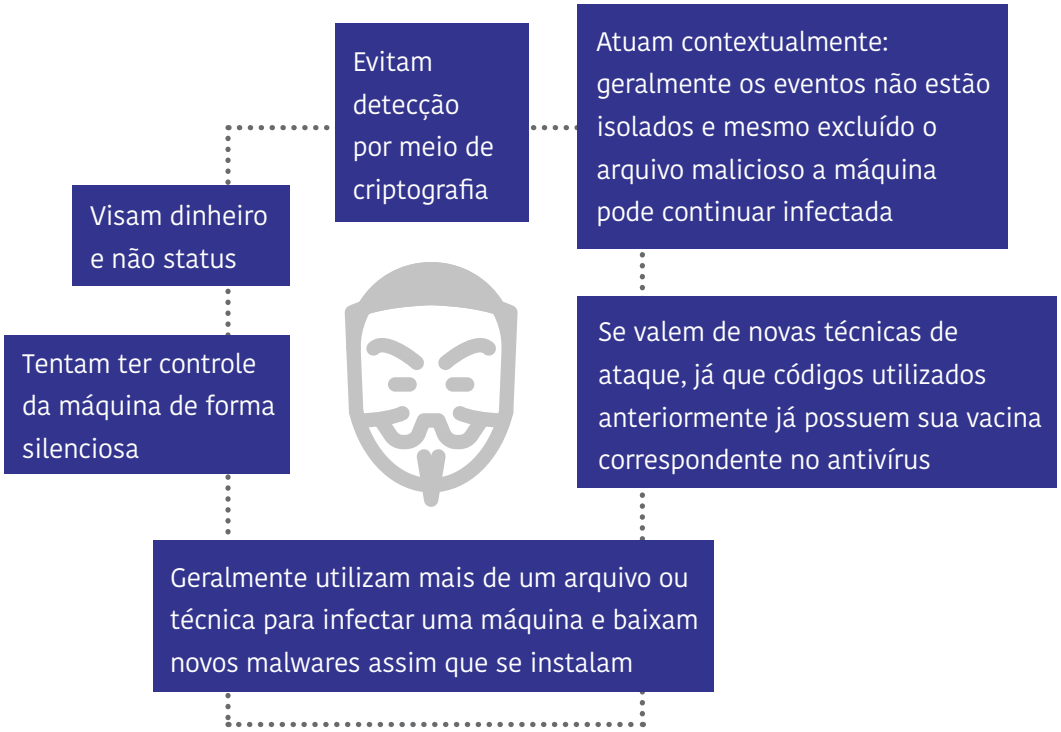
Se não houver atenção a esses pontos, um hacker pode, por exemplo, conectar o notebook à rede e ter acesso ao ambiente LAN (local area network); uma quadrilha especializada pode invadir o sistema de monitoramento e identificar a rotina dos guardas de um banco; e cibercriminosos podem desligar o circuito para que realizem um assalto sem que sejam reconhecidos. Com o uso de software específicos e o investimento em um sistema de vigilância moderno, é possível perceber com mais facilidade uma invasão de algum circuito fechado e, automaticamente, quem o gerencia será alertado dos riscos, podendo mudar chaves de acesso ou, mesmo, excluindo o equipamento de uma rede com internet vulnerável.

4. Falta de gestão e equipe adequada

Há casos em que o problema de segurança da informação não é a tecnologia, mas a falta de pessoal adequado para responder aos alertas feitos pelas ferramentas. Para Taurion, o CIO deve contar com uma equipe que entenda mais do negócio e se envolva em todos os projetos desde o início. A formação desse profissional ainda é muito técnica e há dificuldade em olhar para um projeto de forma estratégica. “Ele precisa entender o objetivo da ação e porque está sendo feita. Só assim consegue desenvolver algo que realmente faça sentido e proteja a empresa”, explica. Outro ponto importante, diz Taurion, é que esses profissionais devem se conscientizar que também fazem parte da companhia, não se colocando em um lugar diferente do usuário.

PERFIL DAS NOVAS AMEAÇAS

As ameaças novas são bem mais complexas do que as antigas. Veja as características que as tornam mais perigosas e difíceis de serem detectadas:



ALÉM DA CRIPTOGRAFIA

A criptografia tem ganhado espaço por três motivos: as empresas precisam proteger sua propriedade intelectual e dados sensíveis; querem preservar a integridade do conteúdo de seus anúncios e projetos, e das análises feitas pelo back-end; e estão investindo mais para proteger a privacidade dos seus clientes. “Ela é importante, mas não a solução dos problemas”, ressalta Fabio Peake, da Cisco. De acordo com ele, a empresa precisa ter dados criptografados, principalmente em ambientes em que eles estão mais expostos, mas não deve ter uma sensação de falsa segurança, negligenciando outras formas de proteção. Peake explica que, em algumas áreas, como em páginas de internet e ambientes públicos, os dados estão mais expostos. De acordo com o estudo da Cisco, muitas das violações mais notáveis nos últimos anos têm aproveitado dos dados não criptografados armazenados nos data centers e outros sistemas internos. Para os criminosos, é como seguir um caminhão blindado de abastecimento em direção a um armazém desprotegido. Também é importante para as organizações entenderem que a criptografia de ponta a ponta pode diminuir a eficácia de alguns produtos de segurança, já que esconde os indicadores de comprometimento usados para identificar e rastrear atividades maliciosas.

4. PAPEL DO CIO

São poucos os CIOs que se veem como líderes da transformação digital e trabalham na conscientização de sua equipe sobre a importância do trabalho colaborativo. “Não há mais espaço para profissionais que trabalham de forma isolada”, afirma Taurion. Segundo ele, o CIO do futuro é o executivo digital. “Ele não pode mais esperar que a empresa defina o que deve fazer – ele precisa estar à frente”, diz. A estratégia de segurança deve se atentar a três aspectos: as tecnologias de segurança necessárias, o perfil de quem cuida dessa área e a conscientização dos funcionários sobre a importância de todos para que os dados estejam seguros. Se, por um lado, o profissional de TI deve começar a entender mais do negócio e se envolver desde o início do projeto, de outro é importante contar com uma prática contínua de assessment - a avaliação constante do ambiente frente ao cenário de ameaças atual, que pode ser diferente a cada semana.

“É essencial um trabalho de atualização de tecnologias de proteção e uma mudança de olhar do profissional de TI, que deve enxergar o negócio como um todo”, afirma Taurion. Segundo ele, a segurança é ainda vista como restritiva ao negócio, aquela que desconfia de todas as inovações e que sempre diz não. “O novo mercado exige essa adaptação dos profissionais, que devem trocar o discurso do ‘não’ pelo ‘como’”, diz Taurion. Para isso, é essencial a integração plena entre as áreas de segurança e de negócios.

Isso passa, também, pelo desenvolvimento de habilidades do profissional, que precisa ser negociador, saber falar numa linguagem apropriada, conhecer mais dos objetivos dos negócios, traçar as opções e explicar os riscos associados para que sejam tomadas as decisões certas e conscientes.

QUESTIONE-SE

O criminoso digital tem várias formas e oportunidades para atacar uma rede ou sistema, mas os defensores da rede têm apenas uma chance e não podem errar. Algumas perguntas podem ajudar o CIO a descobrir o nível de preparo de sua equipe:

5. SOLUÇÕES DA 2S

A perspectiva dos especialistas é que a necessidade de soluções adaptadas e integradas levará a grandes mudanças na indústria de segurança nos próximos cinco anos. Os resultados serão a consolidação da indústria e um movimento unificado em direção a uma arquitetura escalável e integrada de defesas contra ameaças, que fornecerá visibilidade, controle e inteligência.

A seguir, veja os princípios da defesa integrada e as soluções oferecidas pela 2S:

Atuamos no fornecimento de uma arquitetura integrada de segurança, capaz de fechar o cerco e proteger redes, endpoints, sistemas virtuais, data centers, dispositivos móveis, correio eletrônico e gateways de Web. Essa abordagem completa é uma das maiores vantagens do portfólio Cisco.

Assim como o mercado financeiro considera segurança uma premissa do negócio, trabalhamos junto ao cliente para que o tema seja tratado de forma estratégica, em qualquer setor, em qualquer projeto.

Nossos especialistas atuam como consultores estratégicos, apoiando a empresa na identificação dos perfis dos usuários, na construção de uma política adequada para cada um desses públicos e, ainda, na disseminação de uma cultura de segurança na organização.

6. CONTATOS

Renato Carneiro
Presidente

Rodrigo Alves
Engenheiro de Sistemas em Segurança

João Paulo Wolf
Diretor de Soluções e Serviços

www.2s.com.br

INTEGRARE
marketing de conteúdo 360°