SEGURANÇA CIBERNÉTICA GERENCIAR A COMPLEXIDADE

PROTEJA O SEU ATIVO MAIS IMPORTANTE: A INFORMAÇÃO

Segundo a McAfee®, a cada ano são desenvolvidos 60.000.000 programas de malware (software malicioso) à medida que os criminosos cibernéticos continuam desafiando os limites.1 Ainda pior, a espionagem informática suportada pelo setor corporativo e o governo é um problema crescente em escala internacional, pois os hackers utilizam métodos cada vez mais sofisticados para ultrapassar as muralhas da segurança. A proteção dos seus dados é tão importante quanto a proteção do seu dinheiro, já que qualquer situação que coloque em risco os seus sistemas de informação implica também numa ameaça para a sua empresa.

O que aconteceria se a informação confidencial dos seus clientes, membros de agências, documentos financeiros e projetos classificados caíssem nas mão erradas? No melhor dos casos, você poderia perder a sua vantagem competitiva e, num cenário mais pessimista, poderia sofrer perdas significativas. Uma falha na segurança que coloque à sua empresa nas manchetes dos jornais não só danificaria a sua reputação e classificação de crédito, mas também exporia você a ações judiciais e até mesmo à falência.

60 MILHÕES
PROGRAMAS DE MALWARE DESENVOLVIDOS POR ANO POR CRIMINOSOS CIBERNÉTICOS[1]

OS RISCOS DE SEGURANÇA TÊM UM CUSTO MUITO ELEVADO

Os ataques e violações aos seus sistemas de informação resultam caríssimos, seja pelas perdas operacionais que se geram enquanto você se encarrega de identificar e corrigir o problema o pelo tempo e dinheiro que deve investir para recuperar a sua imagem. Se adicionarmos os estritos requisitos de cumprimento que estão sendo aplicados em praticamente todas as indústrias - juntamente com fortes multas e sanções - você notará que o gerenciamento proativo dos riscos pode salvar a sua organização de inumeráveis complicações e custos.

Com uma implementação correta, a Segurança Cibernética permite gerenciar os riscos de maneira proativa. Protege os ativos de informação críticos, garante a integridade dos dados e resguarda a confidencialidade da informação. Além disso, oferece à sua organização a possibilidade de reter provas e iniciar ações judiciais de maneira efetiva.

A SEGURANÇA CIBERNÉTICA PERMITE IMPLEMENTAR POLÍTICAS, PROCEDIMENTOS E MECANISMOS TÉCNICOS PARA PROTEGER, DETECTAR E CORRIGIR PROBLEMAS QUE AMEAÇEM A SEGURANÇA DA SUA REDE.

VOCÊ ESTÁ PREPARADO?

VOCÊ SABIA QUE...?

- Passar de uma rede analógica legada para uma rede digital baseada em IP altamente eficiente aumenta a complexidade e apresenta novos riscos.
- O uso compartilhado de informação e a interoperabilidade geram ainda mais vulnerabilidades.
- O cumprimento normativo e as exigências regulamentares evoluem e costumam estar vinculados com a concessão de financiamento.
- As falhas de segurança podem resultar em publicidade negativa, perdas financeiras e consequências políticas.
- Os orçamentos governamentais diminuem enquanto os requisitos para melhorar a segurança aumentam.

REDES GOVERNAMENTAIS: UM OBJETIVO FREQUENTE DOS HACKERS

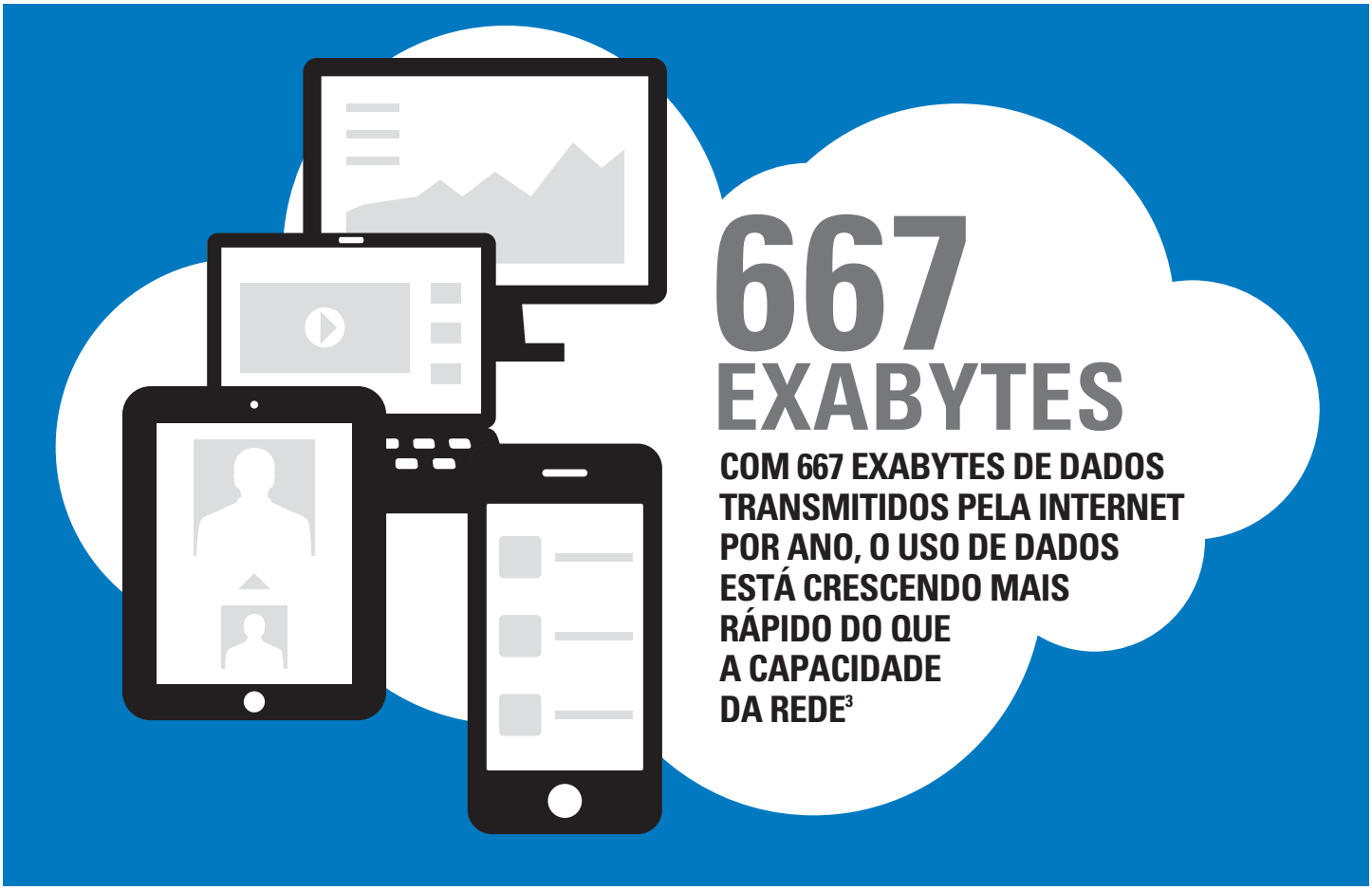
O objetivo dos hackers são as redes governamentais, pois visam conseguir propriedade intelectual muito valiosa. E, com maior frequência, os ataques são originados em países estrangeiros. Um ataque altamente especializado, como o vírus informático Stuxnet, é uma sofisticada ferramenta de ataque cibernético que bloqueou a rede completa de uma planta nuclear e que agora é considerada uma superarma.[2]

A MOBILIDADE IMPLICA UMA MUDANÇA RADICAL E UM DESAFIO PARA TODOS

O avançado poder da computação e a conectividade em qualquer parte estão, literalmente, ao alcance da mão. Os dispositivos empresariais nos permitem estar conectados com smartphones, sistemas de rádios digitais bidirecionais e sistemas de gerenciamento de ativos baseados na localização, e isto contribui para que os trabalhadores móveis possam manter-se em contato com o escritório central. Com as câmeras digitais podemos carregar imagens na nuvem, com os sistemas de jogos temos a possibilidade de competir com jogadores de todo o mundo e com os smartphones ligamos luzes, eletrodomésticos e aparelhos elétricos de maneira remota.

A conectividade em qualquer lugar tem mudado as nossas expectativas do modo em que acessamos a informação no trabalho. O trabalho à distância esta se popularizando. Os dados móveis são ativos de missão crítica. Twitter e Pinterest estão deixando de ser simplesmente um meio social para se tornar ferramentas empresariais. O bloqueio centralizado das redes tornou-se impossível. E o volume de dados está superando a capacidade da rede para gerenciá-los, com 667 exabytes transmitidos anualmente pela Internet até o ano 2013, segundo a Cisco.[3]

Ao mesmo tempo, os empregados levam os seus próprios dispositivos ao trabalho, uma situação que expõe as redes empresariais a um novo mundo de vulnerabilidades. As pessoas tem conseguido um nível de conhecimento tecnológico sem precedentes e cada vez dependem mais dos seus dispositivos móveis. Infelizmente, a maioria desconhece a responsabilidade de proteger os dispositivos e os dados dos que a sua empresa depende, e essa situação representa um enorme risco.



O GASTO COM TI AUMENTA MAS TAMBÉM AUMENTAM AS INTRUSÕES

A maioria das organizações concentram grande parte do seu orçamento de segurança em soluções técnicas. Adquirem o pacote completo (um firewall, um programa antivírus ou uma ferramenta anti-malware), instalam-no na rede e consideram o problema resolvido.

Como os governos estão focalizando um pouco mais sua atenção na segurança da informação, a "aquisição do pacote completo" tem se tornado na "revisão do pacote completo", a fim de garantir que todos os sistemas cumpram com as últimas normas em matéria de segurança de redes.

Qual é a efetividade deste enfoque? Embora 37% das organizações pesquisadas está aumentando o gasto destinado ao cumprimento da segurança da informação e à prevenção de perda de dados e dispositivos móveis, o número de casos de intrusão contínua crescendo.4 Segundo Privacy Rights Clearinghouse (Agência sobre direitos de privacidade), o maior nível de violação de dados foi registrado em 2011 com 535 casos informados que no total, afetaram 30,4 milhões de registros confidenciais. Ainda mais preocupante é o fato de que a maioria desses casos foram gerados por pessoas que pertenciam à organização.[5]

A SEGURANÇA DEPENDE DOS SEUS USUÁRIOS

As más práticas dos usuários podem ultrapassar facilmente o sistema de segurança melhor planejado e mais avançado do ponto de vista tecnológico. Os seus empregados sabem que o fato de sincronizar um smartphone com um PC do escritório ou de usar uma unidade de armazenamento móvel para levar o trabalho da casa ao escritório poderia expor a sua rede aos programas de malware? Eles sabem que o aplicativo não autorizado que instalaram no seu PC do escritório ou a rede ponto-a-ponto utilizada para transferir arquivos grandes poderiam abrir um acesso indireto ao seu sistema cuidadosamente protegido? Eles sabem que se um dispositivo é roubado ou perdido, essa situação poderia comprometer os dados mais confidenciais?

As soluções técnicas e os controles de cumprimento de normas são fundamentais mas nada se compara a um usuário informado e cuidadoso com os temas de segurança. É por isso que implementar processos adequados para que os seus empregados aprendam as melhores práticas de segurança deve ser um tema prioritário. É importante que saibam que utilizar um dispositivo em uma rede sem proteção pode originar uma série de problemas de segurança.

30.4 MILHÕES
DE REGISTROS CONFIDENCIAIS FILTRARAM-SE EM 2011[5]

37%
DAS ORGANIZAÇÕES AUMENTARÁ O GASTO DESTINADO AO CUMPRIMENTO DA SEGURANÇA DA INFORMAÇÃO E À PREVENÇÃO DA PERDA DE DADOS E DISPOSITIVOS MÓVEIS[4]

40% DE AUMENTO
EM ATAQUES CIBERNÉTICOS CONTRA AS REDES FEDERAIS EM UM ANO[6]

9 HORAS PARA CONFIRMAR UMA VIOLAÇÃO[6]

20 HORAS PARA INFORMAR UMA VIOLAÇÃO[6]

MUITAS VEZES A PIOR AMEAÇA NÃO SÃO ELES, MAS SIM NÓS MESMOS

Todas as organizações se defendem "deles", isto é, dos hackers, os espiãs e outras entidades maliciosas que tentam ultrapassar as defensas. Existe um risco menos evidente que tem a ver com os comportamentos arriscados (abrir arquivos anexos, clicar em links, visitar sites Web maliciosos) dos empregados pertencentes à sua organização, mas que o fazem sem nenhuma intenção prejudicial. Até a melhor defesa pode ser quebrada por estes empregados que não seguem as boas práticas de segurança e, negligentemente, deixam o sistema exposto.

Todos "nós", ao fazermos parte de uma organização, devemos compreender quais ativos de informação são armazenados e por que motivo o acesso a esses ativos deve ser limitado. Todos nós devemos confiar em que a informação está protegida. Quanto mais crítica a situação for, mais importante será que o nosso território esteja protegido satisfatoriamente contra todas as ameaças.

O FUNCIONAMENTO EM PILOTO AUTOMÁTICO NÃO É SEGURO

Confiar na "aquisição do pacote completo" ou na "revisão do pacote completo" sem a participação dos usuários é como confiar em um sistema de piloto automático sem a presença de um piloto real no avião. A inteligência artificial não substitui o senso comum de um usuário experimentado. Se a sua empresa só mede o sucesso baseando-se nos resultados da implementação de controles de cumprimento de normas e omite os procedimentos operacionais e as políticas gerenciais, está voando às cegas.

Uma solução de Segurança Cibernética bem sucedida fusiona todos esses aspetos com uma mudança de conduta, em cada nível da organização. Este enfoque, denominado Defesa em Profundidade pela Agência de Segurança Nacional (NSA), é uma estratégia que inclui vários níveis de defesa em todo o ciclo de vida útil do sistema. Leva em conta a tecnologia em uso, as operações da organização e o pessoal que participa no processo.

A empresa se beneficia quando capacita o seu pessoal. Ao insistir constantemente com este tema e ao oferecer capacitação sobre as atuais vulnerabilidades e as melhores estratégias de redução de riscos, você consegue que cada empregado se torne um defensor da segurança. Desse modo, os usuários se transformam em uma ferramenta real para reduzir o custo total de propriedade (TCO). Além disso, este é o primeiro passo fundamental para intensificar a segurança.

OS ATAQUES CIBERNÉTICOS TÊM COMO OBJETIVO AS AGÊNCIAS GRANDES E PEQUENAS. MAIS DE 70 AGÊNCIAS ENCARREGADAS DO CUMPRIMENTO DA LEI FORAM ATACADAS POR UM INFAME GRUPO INTERNACIONAL DE HACKERS, CONHECIDO COMO ANONYMOUS[7]

COMPARTILHAR INFORMAÇÃO É UMA PRÁTICA NATURAL

Muitos dos seus empregados nunca conheceram um mundo sem computadores nem acesso à Internet. Utilizam dispositivos móveis muito poderosos e compartilham dados todos os dias em cada âmbito de suas vidas, seja por meio de álbuns de fotos online, blogs, tweets, cronologias em Facebook ou aplicativos GPS em tempo real.
Quando os empregados possuem acesso à sua intranet ou às suas bases de dados, o fato de compartilhar informação lhes resulta natural. Se eles consideram que a segurança da sua empresa é um obstáculo, costumam evadir esses procedimentos, seja involutária ou intencionalmente. A maioria dos usuários não compreende totalmente os riscos nem é capaz de antecipar as vulnerabilidades. Além disso, como a Segurança Cibernética está geralmente focalizada nos equipamentos de mesa e nos servidores, esquece-se a proteção das tecnologias móveis e portáteis que são as mais utilizadas pelos empregados.

Os especialistas em segurança devem enfrentar o desafio de manter-se atualizados com as crescentes ameaças aos dados digitais, pois os hackers exploram as vulnerabilidades dos novos produtos assim que são lançados ao mercado. O aumento da computação na nuvem adiciona mais outro nível de complexidade para as organizações, já que os usuários compartilham tecnologia, confiam em provedores para a segurança e abrem a organização aos ataques maliciosos perpetrados por hackers capazes de coletar dados confidenciais e de controlar os serviços na nuvem.

QUANTO MENOS SABEM, MAIOR É A AMEAÇA

Os seus empregados talvez não estejam muito bem informados sobre a segurança da informação. Também é possível que a sua organização não tenha definido e implementado políticas de maneira adequada, e que, por sua vez, confie nas medidas de cumprimento de normas, nos mecanismos técnicos ou em uma equipe de TI encarregada da proteção. Ou talvez a causa pode ser a falta de comunicação. Muitos sistemas de segurança não estão documentados ou são percebidos como mandatos sem fundamentos que os usuários omitem facilmente por serem um obstáculo para a produtividade ou por considerá-los diretrizes territoriais do setor de TI.

Uma estrutura informal sem procedimentos claramente documentados pode criar a percepção de que o cumprimento da segurança é opcional. A ausência de um firme respaldo gerencial também pode gerar uma atitude informal que favorece a produtividade em lugar da proteção de dados. Se os tomadores de decisões não priorizam a segurança os usuários também não vão fazê-lo. Finalmente, quanto menos os usuários participarem das políticas de segurança menos responsáveis vão se sentir por seu cumprimento e mais riscos vão assumir involuntariamente.

A SEGURANÇA CIBERNÉTICA É CRÍTICA PARA A CONVERGÊNCIA DE REDES

Independentemente de que a sua agência ou organização utilize um sistema de rádios bidirecionais, o 9-1-1 de próxima geração, um sistema sem fio ou uma rede LTE, existem diversos níveis de complexidade relacionados com cada tecnologia. Como cada nível representa uma oportunidade de que alguem force um controle de segurança e danifique a rede, você necessita diversos níveis de proteção para manter a informação confidencial protegida, desde registros de saúde de pacientes até dados de segurança pública.

Em um panorama que muda vertiginosamente e que se caracteriza por uma combinação de ataques, como vírus, phishing e roubo de identidade, é importante implementar anéis concêntricos de proteção. Este enfoque holístico deve considerar todo o ciclo de vida da proteção da segurança: desde a avaliação da segurança, a integração e os serviços gerenciados - como o supervisionamento do firewall e a proteção contra intrusões - até o desenvolvimento de políticas.

Um erro comum que se repete em muitas organizações é a falta de planejamento. Simplesmente, não é suficiente com implementar um controle de segurança e ficar tranquilo. É preciso realizar uma manutenção e uma revisão dos controles com regularidade, especialmente porque as ameaças ao ambiente mudam continuamente. Além disso, analisar o processo de segurança antecipadamente é fundamental para planejar o seu orçamento.

PERGUNTAS-CHAVE QUE DEVE FAZER PARA PROTEGER A SUA REDE

- Você conta com um programa de segurança estabelecido, com pessoal e fundos designados?
- A sua organização tem atualizado o seu perfil de riscos de segurança?
- Você conta com um programa de gerenciamento de vulnerabilidades?
- Você conta com um procedimento de escalonamento de incidentes?
- As suas redes ou dados estão regulamentados por leis estaduais ou federais?
- Você compartilha informação com outras entidades ou órgãos?

DEFINA OS SEUS OBJETIVOS DE SEGURANÇA, E OS SEUS USUÁRIOS

Quando se trata de Segurança Cibernética, é fundamental definir os seus objetivos e comunicar o seu plano com clareza. Forme uma equipe de usuários e partes interessadas para explorar os objetivos, as realidades, as opções e a vontade das sua organização.

Primeiramente, analise se o objetivo pode ser medido, conseguido e vinculado com a sua missão. Depois pergunte quem são os especialistas internos e os pontos fracos, e qual é a mentalidade dos usuários quanto à segurança. A seguir, pense quais os desafios de segurança que são melhor resolvidos com mecanismos técnicos, mudanças operacionais e conscientização dos usuários, e determine como o orçamento afetará essas alternativas. Finalmente, identifique comportamentos e condições que devam ser mudadas, os recursos requeridos e o valor do suporte externo.

Uma vez definidos os objetivos de Segurança Cibernética pela sua equipe, documente as suas decisões e comprometa-se com um processo contínuo de gerenciamento de mudanças. Para a capacitação, prepare mensagens personalizadas segundo os diferentes usuários da rede.

Assegure-se de utilizar as redes sociais da sua empresa para gerar um consenso e suporte, incluindo a gerencia. Aproveite a experiência dos seus especialistas em segurança internos ou consulte outros que não pertençam à sua organização.

APRESENTE AS SUAS POLÍTICAS E ANALISE OS POSSÍVEIS RISCOS

Quando reúna os seus grupos de usuários, proporcione-lhes políticas claras baseadas em metas e objetivos bem definidos. Indique claramente os riscos que cada procedimento pretende diminuir. Seja sincero e específico ao descrever as possíveis consequências de não cumprir com as normas de segurança.

O seu pessoal deve compreender que os riscos de segurança provêm de fontes internas e externas, de ataques agressivos e vulnerabilidades passivas. Esta é a sua oportunidade de proteger a sua organização das ameaças de engenharia social, como phising e falsificação. Todos devem sair com um ideia clara de como a conectividade à Internet expõe os seus sistemas a ameaças, como cookies, código móvel, ataques de negação do serviço e acessos indiretos a redes ponto a ponto.

DEFINA, DOCUMENTE E DECIDA

A capacitação voltada para a conscientização deve ser um processo contínuo na sua organização se você pretende conseguir uma mudança real no comportamento dos usuários. No caso dos empregados, a documentação é o manual que apoia a aprendizagem deles e define os processos técnicos e os procedimentos operacionais da Segurança Cibernética.

COMO MÍNIMO, A DOCUMENTAÇÃO DEVE TRATAR AS SEGUINTES PERGUNTAS PRINCIPAIS

QUEM DEVE UTILIZAR OS RECURSOS DA REDE?

O acesso se estende a outros órgãos, entidades, provedores externos ou clientes? Deveria se restringir o acesso a determinados grupos de pessoal interno?

QUAL É O OBJETIVO E O PROCESSO DE AUTENTICAÇÃO DE USUÁRIOS?

Quais são as características de uma boa senha e como pode protegê-la? De que maneira a sua organização usa redes privadas virtuais (VPN) e outras ferramentas de autorização remota?

QUE EQUIPAMENTOS PODEM SER CONECTADOS À REDE?

Como está protegida a sua rede contra os sistemas "infectados"?

COMO DEVE SER TRATADA UMA POSSÍVEL FALHA DE SEGURANÇA?

A quem deveria se informar sobre a perda ou roubo de um dispositivo? Qual é o processo para proteger o acesso aos dados quando um empregado é demitido?

AO DESCREVER CLARAMENTE AS FUNÇÕES E AS RESPONSABILIDADES DOS SEUS EMPREGADOS NO PROCESSO DE SEGURANÇA DA INFORMAÇÃO, UMA BOA DOCUMENTAÇÃO CONTRIBUI PARA REDUZIR A CONFUSÃO E MELHORAR A PRODUTIVIDADE. ALÉM DISSO, SERVE COMO NOTIFICAÇÃO DE QUE A SEGURANÇA CIBERNÉTICA É UMA PRIORIDADE PARA A SUA ORGANIZAÇÃO, UM TEMA SUPORTADO PELO ESCALÃO MAIS ALTO E RESPEITADO EM CADA NÍVEL.

PREPARE OS SEUS EMPREGADOS PARA A DEFESA

A conscientização dos usuários é uma importante arma de defesa no seu arsenal de Segurança Cibernética. À medida que o seu pessoal compreenda melhor os riscos e o custo das más práticas, poderá reforçar sua função na proteção da sua organização. Os usuários mais informados podem ser aliados em matéria de segurança, pois eles aceitarão os controles e os aplicarão com maior consistência. Ao compartilhar a responsabilidade de proteger os ativos de informação críticos, os seus empregados são ainda mais valiosos, pois minimizam riscos, reduzem o nível de exposição e diminuem os custos em toda a empresa.

PENSAR LOCALMENTE E AGIR GLOBALMENTE

Os ataques de segurança são cada vez mais imperceptíveis, e costumam ter um objetivo específico, motivados por temas financeiros. Na atualidade, os ataques polimórficos capazes de modificar-se a si mesmos com cada execução são ubíquos. A maioria das organizações gostaria de acreditar que seus dados mais confidenciais e sua informação de missão crítica estivessem imunizados mais isso não é assim. As ameaças são cada vez mais complexas e frequentes, e o fato de investir em tecnologia, respeitar as normas de cumprimento ou instalar uma defesa tradicional no perímetro não é uma solução que garanta a segurança.

À medida que as redes convergem e as pessoas trabalham em colaboração e compartilham dados em todo o mundo, as soluções de Segurança Cibernética devem cobrir todos os aspetos relacionados com as pessoas, políticas, processos e aspetos tecnológicos de maneira global; desde avaliações de segurança de defesa em profundidade até procedimentos para cumprir com os requisitos de cumprimento.

Não há dúvidas que o planejamento adequado é o componente-chave de um enfoque global. Ao detectar e controlar as ameaças desde o começo e implementar novos controles com base nas lições apreendidas de ataques prévios, a sua organização pode adotar uma estratégia produtiva em longo prazo.

ISOLE A SUA REDE E BENEFICIE-SE

Independentemente de se você compartilha dados de segurança pública ou informação de saúde de pacientes ou utiliza uma rede de rádios bidirecionais ou a última rede LTE, ao planejar uma infraestrutura segura e isolar as suas redes com anéis concêntricos de proteção, a sua empresa obtém os seguintes benefícios:

- Maior confiabilidade da rede e melhor cumprimento das normas.
- Eliminação de vulnerabilidades e custos pela interrupção das atividades.
- Melhoria no desempenho dos seus sistemas empresariais críticos.
- Garantia de continuidade das suas operações e da conectividade com o mercado.
- Cumprimento da sua missão e, finalmente, uma ajuda para que a sua organização prospere.

AS SOLUÇÕES DE SEGURANÇA CIBERNÉTICA DEVEM COBRIR TODOS OS ASPETOS RELACIONADOS COM AS PESSOAS, A TECNOLOGIA, AS POLÍTICAS E OS PROCESSOS DE MANEIRA GLOBAL

FONTES

1. Relatório da McAfee sobre ameaças: Primeiro trimestre de 2012
2. "Public safety can benefit when hackers go bad", Urgent Communications, 17 de agosto de 2011
3. "Data, data everywhere", The Economist, 25 de fevereiro de 2010
4. www.eweek.com/c/a/Security/Study-Most-Technology-Companies-Have-Data-Losses
5. www.privacyrights.org/top-data-breach-list-2011
6. www.nextgov.com/technology-news/2011/03
7. "Hacker switches sides to help public safety stave off hack attacks", The Fire Chief, 10 de agosto de 2011

Para saber como gerenciar a complexidade, visite **motorolasolutions.com/services/government**

Motorola Solutions, Inc. 1301 E. Algonquin Road, Schaumburg, Illinois 60196 EE.UU. **motorolasolutions.com**

MOTOROLA