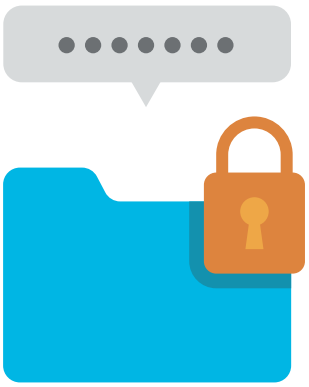
Livro branco empresarial

A segurança começa no terminal

Criar prioridades na segurança de terminais

Elaborado pela

Resumo executivo



82% das organizações depararam-se com uma ameaça/falha em termos de cibersegurança nos últimos 12 meses.[1] O cibercrime está a aumentar em termos de frequência dos ataques, gravidade e custos.

O paradigma da prevenção e proteção da segurança – defender um perímetro de rede com firewall – é coisa do passado. Detetar e responder é bastante mais eficaz.

Mas os orçamentos de TI não conseguem acompanhar a constante evolução da cibersegurança. 77% das despesas ainda são gastas na prevenção e proteção.[2] Apenas 36% dos responsáveis pela segurança das TI sentem que têm um orçamento amplo para garantir uma segurança de terminais eficaz.[3]

É possível proteger os dados de forma robusta. Com a tecnologia adequada – desde soluções de deteção e respostas de segurança a dispositivos individuais –, a estratégia correta e os recursos suficientes, as organizações podem proteger-se do cibercrime.

A incapacidade de aumentar o investimento na cibersegurança e de alinhar o investimento para garantir uma defesa verdadeiramente eficaz resultará em falhas de segurança mais frequentes – e em maiores custos para a organização.

Introdução

A cibersegurança na era das redes amorfas
60% dos líderes de TI afirmam que o aumento do volume e da sofisticação do cibercrime está a superar as suas defesas. 80% dos líderes de segurança afirmam que a ameaça de Ameaças Persistentes Avançadas (APT ou Advanced Persistent Threats), empresas criminosas, hackers e hacktivistas patrocinados por instituições estatais está a aumentar, sendo o maior desafio para a segurança das TI.[4]

E não estão errados. No Reino Unido, o governo afirma que o cibercrime representa um custo económico que ascende a 27 mil milhões de libras, um número que "é significativo e está em crescimento", gerando prejuízos no valor de 21 mil milhões de libras para as empresas.[5] No relatório "State of the Endpoint" (2016) elaborado pela Ponemon, 78% das empresas comunicaram um aumento na gravidade dos ataques de malware, em cerca de 47% em 2011.

Mas o foco nas ameaças externas está errado, e pode conduzir a uma concentração enganosa dos recursos na prevenção e proteção da defesa de perímetros.

Apesar de os ataques externos – vírus, malware, phishing – serem mais comuns, os ataques internos são mais dispendiosos.[6] E muitos desses ataques externos resultam de vulnerabilidades internas; funcionários negligentes que ignoram os protocolos de segurança, dispositivos sem proteção ligados à rede – cerca de 81% dos inquiridos no estudo elaborado pela Ponemon identificaram estes factos como a maior ameaça à segurança das TI.

Isto tornar-se-á cada vez mais real. O terminal é o ponto mais fraco em qualquer rede, e com a ascensão da política BYOD (bring your own device), do trabalho remoto e da Internet das Coisas, os terminais multiplicam-se. Tal significa que o número de portas de entrada para hackers também se multiplica.

Longe das redes antigas controladas de computadores presos a cabos de Ethernet, as redes empresariais tornaram-se amorfas, um emaranhado de dispositivos profissionais e pessoais, com acesso a dados através de várias redes Wi-Fi tanto no local como fora do local.

A situação não é inatacável. Significa simplesmente que se deve adotar uma nova abordagem à cibersegurança. Novas estratégias que respondam à evolução do cibercrime. Uma nova tecnologia que seja capaz de impedir a sofisticação crescente de uma ameaça eminente.

Neste livro branco empresarial, iremos analisar a natureza e a escala da ameaça – por forma a conhecermos melhor o nosso inimigo – antes de abordar a questão de como lidar com a cibersegurança na era dos dispositivos múltiplos, das redes não protegidas e da nuvem.

[1] Estudo "HPI Printer Security" elaborado pela Spiceworks (2016)
[2] Apresentação "Incident Response Management" elaborada pela PAC (2015): https://www.pac-online.com/download/19443/155514
[3] Relatório "State of the Endpoint" elaborado pela Ponemon (2016)
[4] Estudo "CISO Assessment" elaborado pela IBM (2014)
[5] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf
[6] https://digitalguardian.com/blog/insiders-vs-outsiders-whats-greater-cybersecurity-threat-infographic

A escala da ameaça

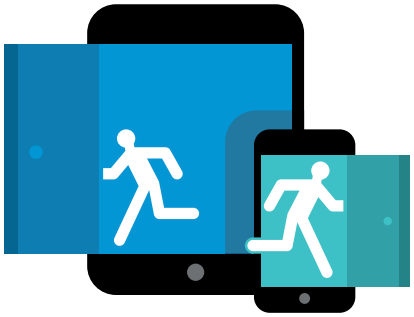
A violação das informações representa para as empresas um custo no valor de 907.053 dólares, com uma perda de cerca de 13% das receitas. Em média, uma empresa demoraria cerca de 9 semanas a recuperar.[7]

Aproximadamente 85% das empresas inquiridas no relatório " Printer Security" (2015) elaborado pela HP afirmaram terem-se deparado com uma ameaça/falha em termos de segurança nos últimos 12 meses. 80% dos profissionais de TI inquiridos preveem que a ameaça aumente nos próximos 3 anos.[8]

O cibercrime tem custos reais. O valor perdido daquilo que é roubado ou danificado. Receitas perdidas decorrentes de danos de reputação e perda de produtividade. Recursos perdidos gastos na recuperação – tempo despendido no suporte, implementação de novas políticas de segurança, perdas de funcionários e outras ações internas. Multas e sanções de entidades reguladoras. Uma queda no preço das ações.

A ameaça vai continuar a crescer juntamente com o número de dispositivos ligados à rede. Com a Internet das Coisas, a Gartner prevê que existam 11,4 mil milhões de dispositivos conectados até 2018, e até 6,4 mil milhões em 2016. Até 2020, mais de 25% dos ataques identificados nas empresas estarão relacionados com a Internet das Coisas, mas a Internet das Coisas abrangerá menos de 10% dos orçamentos de segurança.[9]

A ameaça do cibercrime é grande e está cada vez maior.



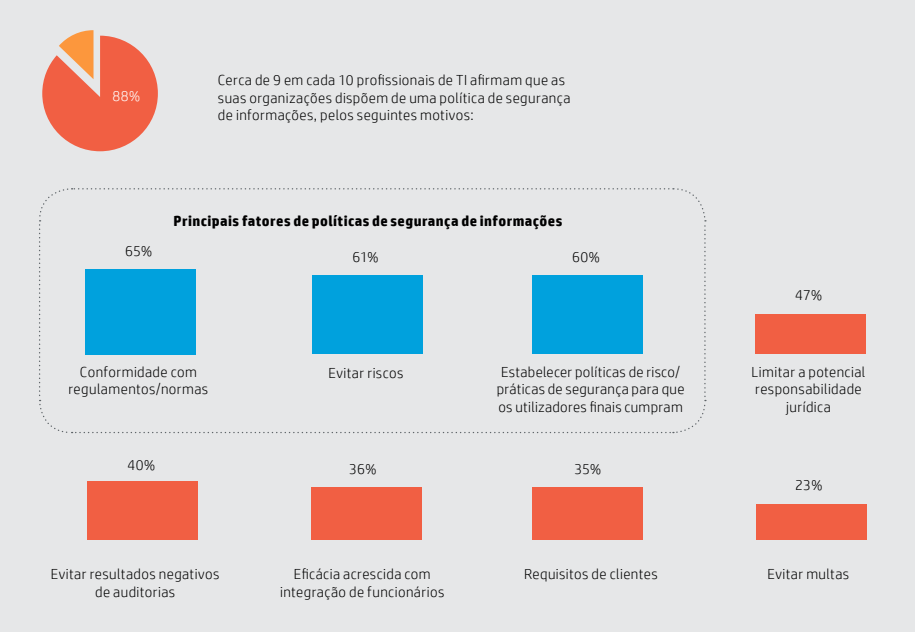
A forma da ameaça

As empresas são afetadas diariamente por inúmeros ciberataques. A maioria são ataques de vírus de nível baixo e ataques de malware. 99% das organizações inquiridas pela Ponemon em 2016 sofreram ataques de malware nos últimos 12 meses. Os ataques externos com base na web como estes são relativamente benignos, tendo um custo médio para as organizações no valor de 4.639 dólares.[10]

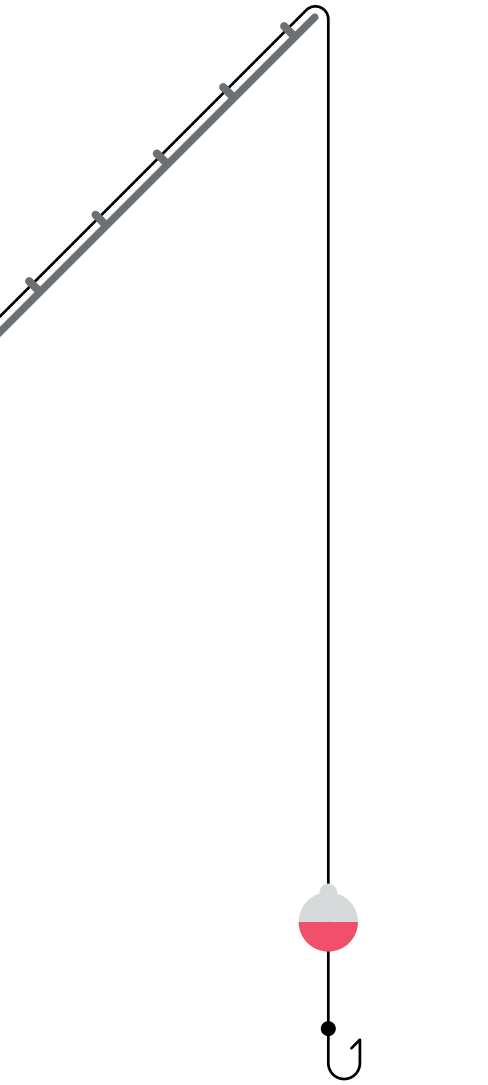
Mas os ataques mais graves são cada vez mais comuns. 51% das organizações inquiridas em 2015 sofreram ataques Direct Denial of Service (DDoS), que podem ser devastadores – tendo um custo médio no valor de 127.000 dólares. O mais alarmante é que 35% das organizações sofreram ataques internos maliciosos, com um custo médio no valor de 145.000 dólares.[9]

A situação emergente é a de ataques permanentes de menor dimensão provenientes do exterior, com ataques menos frequentes mas cada vez maiores; provavelmente, consequência de negligência interna e até mal intencionada. 62% das organizações sofreram ataques de phishing/engenharia social, explorando as fraquezas dos funcionários; isto representa um custo médio no valor de 86.000 dólares.[11]

Um estudo separado realizado pela Spiceworks – em nome da HP – analisou os ataques que 90 organizações no Reino Unido sofreram entre 2014 e 2015.[12]



[7] Relatório "Risk:Value Report" elaborado pela NTT Security (2016)
[8] Relatório "Printer" elaborado pela HP (2015)
[9] http://www.gartner.com/newsroom/id/3291817
[10] https://ssl.www8.hp.com/ww/en/secure/pdf/4aa6-8392enw.pdf
[11] https://digitalguardian.com/blog/insiders-vs-outsiders-whats-greater-cybersecurity-threat-infographic
[12] Estudo "HPI Printer Security" elaborado pela Spiceworks (2016)



Como ocorrem as falhas

As manchetes retratam os hackers a acederem a redes seguras e sofisticadas de governos e empresas, mas a realidade é, normalmente, mais moderada.

Os vírus podem aproveitar-se de redes comprometidas, mas o malware normalmente requer algum tipo de erro por parte do utilizador. Os ataques de phishing/engenharia social dependem disso. Ataques de roubo de informações e ataques DDoS de grandes dimensões são, normalmente, o resultado da negligência do utilizador.

O infame ataque ao Dropbox foi o resultado do descuido de um funcionário da Dropbox que utilizou a mesma palavra-passe para sistemas internos utilizada para a conta do LinkedIn.[13] O alegado ataque russo ao Democratic National Committee (DNC) dos E.U.A. foi, aparentemente, devido a John Podesta, antigo conselheiro da Sr.ª Clinton, que clicou erradamente num e-mail de phishing identificado como "legítimo" por um assistente.[14]

Os hackers não precisam de assistência ativa para terem êxito nas suas missões e ataques. Tão perigoso quanto a ignorância é desrespeitar os protocolos de segurança. Uma ameaça crescente é a de os funcionários trazerem os seus próprios dispositivos para o local de trabalho, usando software de nuvem comercial, ambos criando elementos inseguros numa rede segura; fora do controlo das TI da empresa, o que gera vulnerabilidades.

A maioria das vezes, os hackers não precisam de implementar algoritmos sofisticados ou tecnologia de ponta, precisam simplesmente que alguém seja ligeiramente descuidado ou distraído.

A firewall pertence ao passado

O pilar da cibersegurança era, até há pouco tempo, o antivírus e o software de firewall. Prevenir e proteger. Criar um perímetro seguro. No ambiente de trabalho atual, esta não é simplesmente uma estratégia credível.

81% dos inquiridos pela Ponemon afirmam que os dispositivos móveis na sua rede foram alvo de malware. Outros aumentos nos riscos de segurança incluem a utilização de aplicações de nuvem comerciais – afirmam 72% dos inquiridos –, BYOD (69%) e funcionários que trabalham partir de escritórios em casa e locais remotos (62%).[15]

Dito de uma forma simples, uma firewall fazia sentido quando, como administrador de rede, era possível controlar os dispositivos aos quais estava conectada. Mas numa era em que os funcionários trazem os seus próprios dispositivos para o local de trabalho – muitas vezes vários e sem o devido conhecimento do departamento de TI – e com o número crescente de funcionários que se conectam de forma remota, torna-se impossível proteger o perímetro. Cada dispositivo não aprovado é um terminal vulnerável para os hackers explorarem.

[13] https://www.theguardian.com/technology/2016/aug/31/dropbox-hack-passwords-68m-data-breach

[14] https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html?_r=0

[15] Relatório "State of the Endpoint" elaborado pela Ponemon (2016)

A perspetiva da HP: ir mais além da segurança da rede

Michael Howard, diretor global de práticas de segurança da HP, fala sobre garantir a segurança dos terminais.

Uma preocupação atual e fundamental é o facto de as empresas se esforçarem para manter cada terminal seguro devido à falta de consciência e de conhecimento sobre determinados dispositivos e riscos associados. As empresas sentem-se seguras por detrás de uma firewall, apesar de esta já não ser suficiente para protegê-las de ataques. As equipas de segurança devem conhecer cada terminal na infraestrutura e garantir que cada terminal tem diversas camadas de proteção para proteger de ataques cada vez mais sofisticados.

É essencial que as equipas de segurança investiguem cada canto da infraestrutura de TI da sua empresa e criem uma camada adicional de proteção para além dos perímetros da rede convencionais. As firewalls por si só não conseguem resistir aos ataques sofisticados, e uma política de defesa com diversas camadas de proteção em cada terminal é essencial para garantir que a sua empresa consegue cumprir os requisitos regulamentares e evitar multas dispendiosas.

A política da HP é que, em cada nova solução, serviço ou produto que desenvolvemos, a segurança esteja em primeiro lugar. As equipas de desenvolvimento sabem que devem abordar as questões de segurança e que devem saber como colocar essas questões na rede de uma forma segura.

Mais do que nunca, a segurança deve estar em primeiro lugar. Esta tem sido a política da HP durante anos.

Segurança por camadas

Uma nova abordagem à cibersegurança tem de ser por camadas.
A segurança da rede ainda é importante, mas deve ser composta por redes discretas. Muitas falhas residem numa entrada inicial que garante o acesso a tudo o que existe no sistema. Pense no erro de phishing de John Podesta. É essencial proteger as informações confidenciais em várias categorias de acesso, para que roubar uma única chave não signifique controlar e apoderar-se de tudo o resto.

Os dispositivos devem ser tidos em conta. Uma questão fundamental para os gestores de TI é garantir que cada dispositivo conectado à rede está protegido por um software de segurança regularmente atualizado – contra vírus, malware e spyware – e é regularmente analisado para detetar anomalias. O melhor é usar os próprios dispositivos como sensores, recolhendo informações em tempo real para alertar relativamente a eventuais falhas no perímetro da rede da qual fazem parte.

Uma governança de segurança abrangente deve estar em vigor, e todos os funcionários devem estar formados em protocolos de cibersegurança. O erro humano – desde clicar na hiperligação errada a conectar um dispositivo de consumidor – é a ameaça número um para as redes. O erro humano pode ser reduzido com a formação adequada.

Segurança dos dispositivos

Talvez a questão principal no confronto com a cibersegurança contemporânea seja controlar quais os dispositivos que têm acesso à rede.
A primeira solução normalmente adotada é ter redes Wi-Fi separadas para visitantes e funcionários, para que os dispositivos externos não protegidos não acedam à rede principal. Este facto está diretamente relacionado com a formação dos funcionários para que utilizem esta rede nos seus dispositivos pessoais.

A segunda solução é garantir que controla os dispositivos dos seus funcionários. Esta questão deve ser abordada na política da empresa em termos de BYOD (bring your own device) e CYOD (choose your own device) e é um forte argumento a favor do CYOD – dando mais controlo em termos de que dispositivos são usados, escolhendo aqueles que têm melhores funcionalidades de segurança, a forma como estão configurados e a gestão e monitorização destes dispositivos.

Usar um dos nossos PC da gama HP Elite, por exemplo, é preferível a usar um computador portátil mais económico. Cada PC HP Elite incorpora a tecnologia HP SureStart que verifica o BIOS a cada 15 minutos e reconfigura a máquina para o seu estado inicial ao detetar uma anomalia, bloqueando intrusos. Graças a esta funcionalidade – e a muitas outras – os nossos computadores HP Elite série 800 foram recentemente considerados "os PC mais seguros do mundo".[16] Mas é pouco provável que os funcionários tenham um PC HP Elite.

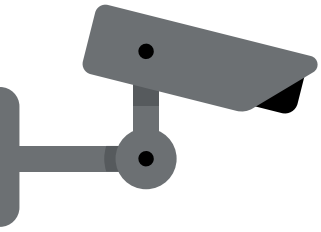
Normalmente, os funcionários preferem usar os seus próprios dispositivos por dois motivos:
1. A tecnologia de consumidor é normalmente melhor do que aquela fornecida pelo local de trabalho.
2. Os funcionários gostam de utilizar tecnologia com a qual estejam familiarizados.

Ao implementar uma política CYOD com bons recursos, que ofereça os dispositivos mais recentes dentro de um ciclo de atualizações regulares, as organizações podem fornecer melhores dispositivos do que aqueles que os funcionários possuem, e manter um maior controlo sobre a segurança de tais dispositivos. É por isso que comercializamos o nosso produto como HP Device as a Service (DaaS).

É essencial incluir todos os dispositivos na estratégia de segurança, mesmo aqueles que são frequentemente esquecidos. Num inquérito da IDC, 80% dos inquiridos afirmaram que a segurança das TI é importante para as respetivas empresas, mas apenas 59% consideraram a segurança de impressoras um elemento importante, apesar de mais de metade ter sofrido falhas de segurança envolvendo impressoras nos últimos 12 meses. Trata-se, claramente, de um ângulo morto.

O número médio de falhas de segurança antes de implementar uma política de segurança de impressoras era de 9,9 por ano, representando um custo médio no valor de 521.400 dólares (incluindo multas). Após a implementação da segurança de impressoras, o número médio de falhas desceu para 1,5, poupando 200 horas de tempo dos funcionários por ano e 250.000 dólares em custos associados, incluindo auditoria e conformidade.[17]

[16] http://www8.hp.com/us/en/campaign/computersecurity/
[17] Relatório "The Business Value of Printer Security" elaborado pela IDC (2015)



Deteção e resposta pró-ativas

77% do orçamento de segurança das TI é despendido em tecnologia de prevenção e proteção como software antivírus e firewalls, de acordo com um estudo realizado pela PAC. Mas esta abordagem não é eficaz. O estudo também demonstra que 67% das empresas inquiridas já sofreram uma falha cibernética nos últimos 12 meses, e 100% já passaram por tal situação no passado.[18]

O software antivírus, em especial, é incrivelmente ineficaz. A Damballa realizou testes nos quais atacava deliberadamente uma rede para analisar a capacidade de resposta do antivírus. Demorou mais de 6 meses para que 100% dos ficheiros maliciosos fossem identificados.[19] Isto coincide com uma outra conclusão da PAC, que demonstrou serem necessários entre 1 e 6 meses para que as empresas descobrissem que tinham sido atacadas.

Manter os terminais seguros não pode depender apenas da prevenção. O número crescente de incidentes com vírus/malware, para além da insegurança inerente ao trabalho BYOD/móvel significa que as falhas são inevitáveis. Ninguém está a sugerir que a prevenção e a proteção sejam completamente esquecidas, mas é óbvio que a deteção e resposta têm de estar mais no centro das atenções.

É necessária uma monitorização contínua e em tempo real, idealmente usando os próprios terminais como sensores – alertando o resto da rede quando estes são atacados. Isto permite respostas remotas da parte da segurança de TI, incluindo processos como:

- Desligar o dispositivo de forma remota.
- Cancelar um processo infetado ou um processo que esteja a espalhar malware.
- Colocar em quarentena um ficheiro específico ou um grupo de ficheiros.
- Interromper as comunicações da rede para isolar os dispositivos infetados.[20]

Aceitar que as falhas vão acontecer e pôr em prática os devidos protocolos de resposta – assim como implementar a tecnologia necessária para os executar – é a única forma de garantir a cibersegurança, quando já não podemos depender apenas da prevenção.

"A tecnologia não pode ser segura se as próprias pessoas a comprometem."

– Joseph Steinberg [21]

Segurança dos funcionários

Igualmente importante, senão mais importante do que manter o dispositivo seguro, é manter segura a pessoa que o utiliza.
Cada funcionário deve ter formação em cibersegurança. Os funcionários devem estar cientes dos riscos de phishing. De navegar em websites suspeitos. Ou de descarregar anexos suspeitos. Devem ter conhecimento da política de palavra-passe segura – usando palavras-passe fortes, únicas para cada início de sessão, e usando o gestor de palavras-passe adequado para as armazenar.

Devem estar cientes da importância de manter o software de segurança dos seus dispositivos regularmente atualizado, para facilitar a tarefa de monitorização do departamento de TI. Devem estar atentos e usar apenas dispositivos seguros para aceder às redes da organização e evitar usar dispositivos pessoais em redes externas, não protegidas para aceder a dados confidenciais.

Muitos especialistas em cibersegurança recomendam a realização de simulações de ataques de phishing – criando websites de phishing falsos para testar os funcionários – e levando a formação em cibersegurança a um nível mais formal. Isto é fundamental, porque a maioria dos ataques depende da fraqueza humana, seja por negligência, seja por malícia.

E porque as pessoas são o elo mais fraco em qualquer rede.

[18] Apresentação "Incident Response Management" elaborada pela PAC (2015)
[19] https://www.damballa.com/time-to-fix-malware-strategies-2/
[20] "The Essential Endpoint Detection Checklist" – HP Now
[21] https://digitalguardian.com/blog/data-security-experts-answer-what-biggest-misconception-companies-have-about-endpoint-security

Conclusão

As despesas em segurança das TI devem transitar da prevenção e proteção para a deteção e resposta no terminal.
Proteger os dados de uma organização no clima atual de TI – face a uma ameaça de cibercrime crescente e a uma perda de controlo do perímetro da rede – requer duas coisas: uma transição conceptual e mais recursos.

O conceito de rede tem de mudar. A ideia de uma rede como uma vedação em torno de um conjunto de dispositivos deixou de se aplicar. Chegou o momento de reconhecer a realidade. "A rede" é uma quimera. Emerge dos dispositivos conectados – cada um deles sendo um terminal. Manter uma rede segura significa manter um terminal seguro. E cada terminal é composto por dois elementos: o dispositivo e a pessoa que o utiliza. Ambos devem ser tidos em consideração.

Mas impor a segurança neste novo paradigma é muito mais complicado do que um ambiente simples de computadores conectados por Ethernet do passado. Requer mais recursos e estes devem ser impulsionados. Cerca de 61% dos inquiridos pela Ponemon reconhecem tal.

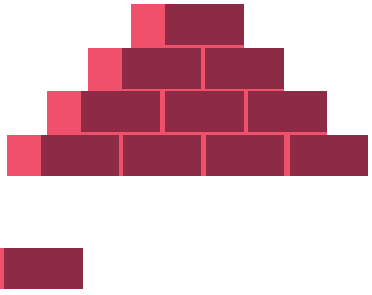
A parte mais complicada é envolver toda a organização no processo. Apenas 36% dos inquiridos afirmam que dispõem de um orçamento vasto e de funcionários que garantem a segurança dos terminais. 69% dos inquiridos afirmam que o departamento de TI não consegue suportar a exigência dos funcionários de um maior apoio. 71% dos inquiridos afirmam que as políticas de segurança dos terminais são difíceis de executar.[22]

80% dos gestores de TI consideram que a conformidade regulamentar é a melhor forma de justificar o financiamento dos seus programas de segurança, mas também consideram que a conformidade é o motivo menos importante para incorrer em despesas. A conformidade significa cumprir os requisitos mínimos.[23]

Os decisores de TI devem dialogar com os executivos para destacar a importância da segurança. Torne óbvios quais os custos de uma segurança negligente e descuidada – as despesas de recuperação, as receitas perdidas, a queda do valor das ações – e reforce as poupanças a longo prazo. Muitas soluções de segurança também geram melhorias gerais. Pense na produtividade acrescida ao implementar benefícios de segurança de impressão e produtividade ao fornecer tecnologia regularmente atualizada num programa CYOD flexível disponibilizado por terceiros com base numa subscrição (como o HP DaaS). É possível criar um caso empresarial claro e sólido.

O desafio é impressionante. E com o tempo – com a explosão de dispositivos na era da Internet das Coisas, e a crescente sofisticação do cibercrime – apenas se tornará mais assustador. Mas não é insuperável. Com a tecnologia certa, a estratégia certa e os recursos certos, podemos defender os nossos terminais. Podemos manter os dados seguros.

Para saber mais informações sobre o HP Device as a Service e sobre como este pode ajudar a desenvolver um programa CYOD abrangente e flexível, visite-nos ao clicar **aqui.**



Subscrever atualizações
hp.com/go/getupdated

Partilhar com colegas

Classificar este documento

4AA7-1089PTE

[22] Relatório "State of the Endpoint" elaborado pela Ponemon (2016)
[23] https://www.sans.org/reading-room/whitepapers/analyst/security-spending-trends-36697