Economias Clandestinas

Capital intelectual e dados corporativos confidenciais são agora a mais nova moeda do cibercrime

McAfee | SAIC

Economias Clandestinas

Capital intelectual e dados corporativos confidenciais são agora a mais nova moeda do cibercrime

Conteúdo

Prefácio de Simon Hunt, vice-presidente e executivo-chefe de tecnologia de segurança de terminais da McAfee

A globalização e a mercantilização (commoditization) da tecnologia da informação levaram as empresas a armazenar volumes crescentes de dados corporativos críticos e valiosos na nuvem. Enquanto essa mudança ocorria, os cibercriminosos descobriam novas maneiras de chegar a esses dados valiosos, tanto de dentro quanto de fora da empresa.

No passado, os cibercriminosos visavam informações pessoais, como números de documentos ou de cartões de crédito, os quais eram vendidos no mercado negro. Agora, esses criminosos compreendem que há muito mais vantagens em vender informações pertencentes a uma empresa para concorrentes e governos estrangeiros. Por exemplo, os documentos jurídicos de uma empresa podem valer muito mais do que uma lista de cartões de crédito de clientes.

A economia do submundo cibernético mudou seu foco para o roubo de capital intelectual corporativo - a nova moeda do cibercrime. O capital intelectual engloba todo o valor que uma empresa deriva de sua propriedade intelectual, incluindo segredos comerciais, planos de marketing, descobertas de pesquisa e desenvolvimento e até mesmo código-fonte. A Operação Aurora, por exemplo, um ataque dirigido contra o Google e pelo menos 30 outras empresas, representou um ataque sofisticado concebido para roubar capital intelectual.

Mais recentemente, descobrimos os ataques 'Night Dragon' (Dragão Noturno) contra empresas de gás e petróleo de todo o mundo que, ao longo de um período de vários meses, surrupiou de maneira discreta e insidiosa vários gigabytes de informações internas altamente confidenciais, incluindo informações proprietárias sobre operações de campo, financiamento de projetos e documentação de licitações. Embora esses ataques fossem voltados especificamente para o setor energético, as ferramentas e técnicas utilizadas podem ser muito bem-sucedidas em ataques a outras indústrias.

Agora, as soluções de proteção de dados são mais importantes do que nunca, pois as ameaças podem vir tanto interna quanto externamente à empresa. O WikiLeaks, por exemplo, representa uma nova ameaça às empresas, pois pessoas de dentro ficarão cada vez mais tentadas a divulgar os segredos de suas empresas em troca de ganhos financeiros ou tecnológicos, para aumentar o nível de transparência das empresas ou para expor o que eles acreditam ser irregularidades. A enxurrada de publicidade recente em torno do WikiLeaks fez com que as empresas reconsiderassem seriamente o que é confidencial, o que deve ser público e o que deve ser protegido. Com a contínua diluição do perímetro das empresas devido à extensão de operações a dispositivos móveis, computação em nuvem e fornecedores terceirizados, a contenção dos vetores de intrusão está se tornando cada vez mais difícil. Uma vez concluída a exploração da rede, a economia clandestina é muito competente no roubo e monetização dos dados.

Embora os investimentos em segurança de TI (Tecnologia da Informação) estejam aumentando para evitar esses roubos de capital intelectual, o grau de sofisticação dos ataques também aumenta, o que exige soluções e tecnologias avançadas, além de treinamento e políticas, para neutralizar as ameaças. Ter políticas implementadas é importante, mas as políticas, isoladamente, não estão resolvendo o problema.

Este relatório avalia o estado global da segurança corporativa, sobre a qual se observa certo despreparo quanto à proteção contra a sofisticação dos ataques gerados pela economia clandestina. Estariam as empresas com políticas adequadas e com abordagens voltadas para esse cenário? O relatório conclui com abordagens para proteção de capital intelectual com o objetivo de conter as perdas e aproveitar plenamente a recuperação econômica.

Introdução

Dois anos atrás, a McAfee elaborou o relatório Economias Desprotegidas, o primeiro estudo global sobre a segurança das economias da informação. Aquele estudo revelou, com base em uma pesquisa global, que empresas do mundo inteiro perderam um valor estimado em US$1 trilhão em 2008 devido a vazamentos de dados, custos de correção e danos à reputação. Hoje, na medida em que a economia mundial começa a se recuperar, empresas de todo o mundo estão reavaliando seu capital intelectual e o quanto é gasto devido a perdas de dados e ataques cibernéticos. O capital intelectual engloba todo o valor que uma empresa deriva de sua propriedade intelectual, incluindo segredos comerciais, planos de marketing, descobertas de pesquisa e desenvolvimento e código-fonte.

A Internet derrubou as fronteiras geográficas e as empresas têm muito de seu valor em informações intangíveis armazenadas na nuvem. Ao buscar novas informações para roubar, os cibercriminosos examinam questões, como armazenamento no exterior, que tornaram o roubo de capital intelectual mais predominante e o processo criminal muito mais difícil. Frequentemente as empresas não estão nem mesmo cientes de que suas informações estão sendo roubadas devido à sofisticação dos tipos de técnicas utilizadas.

Embora os aspectos geográficos e culturais possam desempenhar sua parte, particularmente em países nos quais os limites entre empresas e governo são tênues, é o valor dos dados que determina quem e o quê será atacado. O alvo e a motivação são quase sempre financeiros.

Em 2011, muitas questões serão semelhantes àquelas levantadas há dois anos, mas a recuperação econômica, contrastando com a crise econômica, torna o contexto diferente. Como a recuperação econômica afetará a capacidade das empresas de proteger informações vitais? Quais países representarão a maior ameaça à estabilidade econômica de outros países? Como os cibercriminosos atingirão corporações além de todas as fronteiras? Como a proteção de ativos digitais ajudará ou prejudicará a recuperação econômica global no ano que começa?

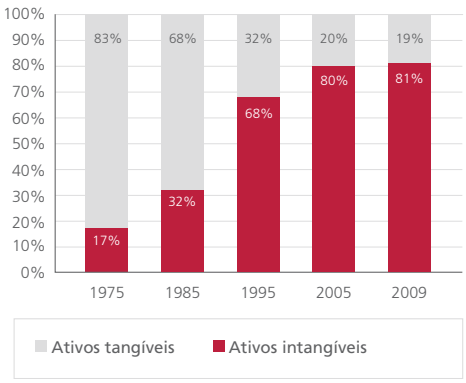
Em colaboração com especialistas das áreas de proteção de dados e propriedade intelectual, a McAfee e a Science Applications International Corporation (SAIC), uma empresa de aplicações científicas, tecnológicas e de engenharia listada na FORTUNE 500®, analisaram detidamente essas questões.

Através de uma pesquisa com mais de 1.000 tomadores de decisões de TI seniores dos Estados Unidos, Reino Unido, Japão, China, Índia, Brasil e Oriente Médio, a McAfee, juntamente com a SAIC, desenvolveu um estudo sobre esse tópico. A pesquisa, realizada pela empresa internacional de pesquisa Vanson Bourne, revela as mudanças de atitude e percepções da proteção à propriedade intelectual nos dois últimos anos.

Seção 1: A mudança na economia e o valor da propriedade intelectual

A economia teve uma mudança nos últimos 20 anos, de ativos físicos como representação principal do valor, para o capital intelectual representando o grosso do valor corporativo. Uma análise recente da Ocean Tomo Intellectual Capital Equity estima o valor das intangibilidades em aproximadamente 81% do valor das empresas S&P 500 – uma parcela significativa do que é representado por tecnologia patenteada, segredos comerciais, dados proprietários, processos comerciais e planos de entrada no mercado.

Componentes do valor de mercado da S&P



FONTE: OCEAN TOMO

É frequentemente difícil determinar o valor do capital intelectual porque o mesmo é raramente avaliado, às vezes se beneficia de anos de investimento direto e indireto e a demanda da economia clandestina estabelece um preço que costuma não refletir com precisão seu valor para a empresa à qual ele pertence. Por exemplo, a atual fórmula da Coca-Cola pode não ser tão valiosa para um concorrente quanto o plano da corporação Coca-Cola para sua nova linha de produtos. O que são uns poucos milhões de dólares se uma empresa concorrente pode economizar bilhões em pesquisa e desenvolvimento roubando dados de propriedade da Coca-Cola? Marcel van den Berg, da Team Cymru, define a ameaça da seguinte forma:

"Tudo que pode ser monetizado pode se tornar alvo da economia clandestina. Isso varia de credenciais bancárias de indivíduos a cópias de bancos de dados de empresas Fortune 100.

"Tudo que pode ser monetizado pode se tornar alvo da economia clandestina. Isso varia de credenciais bancárias de indivíduos a cópias de bancos de dados de empresas Fortune 100."

Marcel van den Berg, da Team Cymru.

"Em alguns casos, governos apoiam o roubo de segredos comerciais e, em alguns países, os limites entre empresas e governo são tênues. Se os custos de pesquisa e desenvolvimento são mínimos ou inexistentes, as empresas podem colocar produtos no mercado mais rapidamente e auferir grandes lucros com os investimentos de outras empresas. O roubo de capital intelectual pode significar o fim de uma corporação e empresas do mundo todo devem se preocupar com isso.

Em 2009, o oficial alemão Walter Opfermann, especialista em proteção contra espionagem no escritório de contrainformação do estado de Baden-Württemberg, afirmou que a China estava utilizando uma série de "métodos refinados", de espiões tradicionais a escutas telefônicas e cada vez mais a Internet, para roubar segredos industriais.[1] Os setores mais atacados foram fabricação de automóveis, energias renováveis, química, comunicações, ótica, tecnologia de raios X, máquinas, pesquisa de materiais e armamentos. Os cibercriminosos obtêm informações sobre pesquisa e desenvolvimento, técnicas de gerenciamento e estratégias de marketing.

Na Itália, em setembro de 2010, o ex-engenheiro da Ferrari Nigel Stepney foi sentenciado a 20 meses de prisão por seu papel no vazamento de dados corporativos confidenciais em 2007. Stepney foi considerado culpado de "sabotagem, espionagem industrial, fraude desportiva e lesão corporal premeditada", por ter passado dados técnicos da Ferrari para a equipe de corridas rival McLaren.[2]

O roubo de capital intelectual pode significar o fim de uma corporação e empresas do mundo todo devem se preocupar com isso.

O capital intelectual está cada vez mais vulnerável devido à convergência entre empresas e TI. Os segredos comerciais e dados proprietários residem em bancos de dados e são compartilhados por e-mail e pela Internet. Os alvos da economia clandestina mudaram significativamente nos últimos anos. Embora o roubo e venda de cartões de crédito roubados ainda seja uma atividade rentável, o capital intelectual tornou-se recentemente a nova fonte de dinheiro grande e fácil.

De fato, os vetores e alvos dos ataques virtuais na atual sociedade da informação em rede estão se multiplicando. A Comissão de Crimes de Alta Tecnologia da OAB – SP resume da seguinte forma: "Estamos vendo grupos especializados em tornar indisponíveis redes, serviços e infraestruturas básicas utilizando ataques mais sofisticados (DDoS) e causando perda de lucros e danos à imagem de grandes corporações. Por outro lado, existem grupos voltados para a busca de informações confidenciais e espionagem industrial. Os vazamentos de dados governamentais serão uma constante."

Atualmente, os cibercriminosos procuram conteúdo por lucro e podem se movimentar com rapidez e flexibilidade para atingir seus objetivos. Assim que uma vulnerabilidade é identificada, eles organizam uma grande operação em poucos dias após sua descoberta. Eles desenvolvem uma exploração e roubam tantos dados úteis quanto

possível em um breve período de tempo. Mulas são, então, utilizadas para enviar os lucros (após descontar uma comissão) para os líderes do submundo.

A economia do armazenamento de dados no exterior está desempenhando um papel mais importante na tomada de decisões na medida em que o armazenamento no exterior se torna mais barato e as empresas percebem a vantagem que isso pode representar para sua lucratividade. Mais de metade das empresas estudadas estão reavaliando os riscos do processamento de dados fora de seus países de origem devido à crise econômica, em comparação com quatro em cada dez que o faziam em 2008.

Fragmentos de e-mail que descrevem cultura corporativa, manuais de funcionários e patentes são os tipos de dados menos protegidos. Um quarto ou mais das empresas afirmam estar alocando muito pouco ou nenhum orçamento para a proteção desses dados. Dados de clientes/fornecedores, dados de funcionários e segredos comerciais são os dados melhor protegidos, embora ataques cibernéticos, como a Operação Aurora (e outros), provam que os segredos comerciais mais cobiçados estão ao alcance de atacantes sofisticados, apesar das proteções de segurança tradicionais.

Tanto o valor das informações quanto a quantia gasta na proteção das informações diminuíram nos últimos dois anos. Em 2008, as empresas gastavam quase US$ 3 na proteção de US$ 1 de dados. Proporcionalmente, houve um aumento para US$ 4,80 em segurança para cada US$ 1 de dados armazenados no exterior porque muitas empresas reduziram a quantidade de dados armazenados no exterior, mas mantiveram as mesmas proteções. Ao mesmo tempo, aproximadamente um terço das empresas tem procurado aumentar a quantidade de informações confidenciais que armazenam no exterior, enquanto há dois anos era uma em cada cinco empresas.

Alguns países tornam mais fáceis o armazenamento no exterior porque suas leis sobre privacidade e notificação são muito brandas. Oito em cada dez empresas que armazenam informações confidenciais no exterior são influenciadas por leis de privacidade que exigem notificação de violações de dados aos clientes. Sete em cada dez empresas que armazenam informações confidenciais no exterior o fazem em países nos quais as leis lhes dão mais autonomia.

Decisões com o objetivo de proteger informações confidenciais são frequentemente tomadas para manter conformidade com os regulamentos do país. No entanto, apenas pouco mais de um terço das empresas considera que os regulamentos de conformidade impostos por seus países de origem são suficientemente úteis e vão fundo no cerne do problema para proteger o capital intelectual da corporação.

Aproximadamente um terço das empresas tem procurado aumentar a quantidade de informações confidenciais que armazenam no exterior.

Seção 2: A proteção de dados confidenciais

Houve uma evolução no submundo cibernético, o tipo de dados visado pelos ataques mudou e conforme os ataques se tornaram mais sofisticados, a abordagem à proteção de dados também mudou. As empresas não apenas precisam se preocupar com o roubo de capital intelectual cometido, mas devem também se preocupar com informações importantes ou mesmo confidenciais que podem vazar para a mídia, como no caso do WikiLeaks.

Em julho de 2010, Gordon M. Snow, diretor assistente do FBI, testemunhou perante o subcomitê judiciário sobre crime, terrorismo e segurança interna (House Judiciary Subcommittee on Crime, Terrorism, and Homeland Security).

"O impacto do crime cibernético sobre os indivíduos e o comércio pode ser significativo, com consequências que vão desde uma mera inconveniência à ruína financeira. A possibilidade de lucros consideráveis é tentadora para os jovens criminosos e isso resultou na criação de uma grande economia clandestina conhecida como submundo cibernético. O submundo cibernético é um mercado difundido, governado por regras e uma lógica muito semelhantes às do mundo dos negócios legítimos, incluindo uma linguagem própria, um conjunto de expectativas sobre a conduta de seus membros e um sistema de estratificação com base em conhecimentos e habilidades, atividades e reputação."

A persistência e a sofisticação das novas ameaças são significativas e os ataques ocorrem mundialmente. Em novembro de 2010, a Postmedia News informou que 86% das grandes corporações canadenses tinham sido atacadas, segundo um relatório secreto do governo canadense. O relatório também afirmou que o "hacking" de espionagem do setor privado tinha dobrado em dois anos.

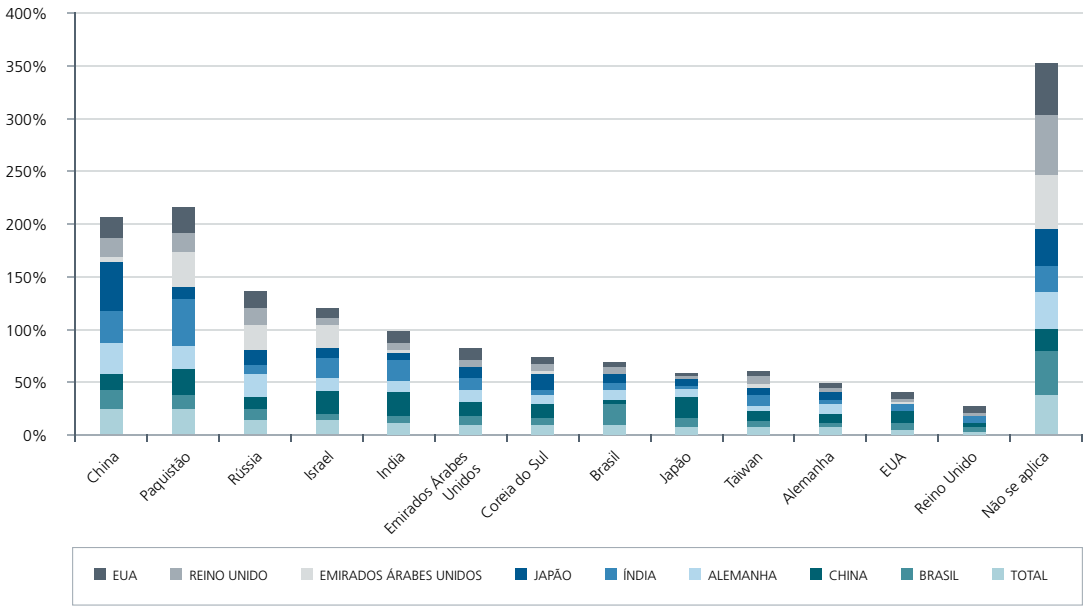
Um relatório da Forrester Research de março de 2010 constatou que conhecimentos proprietários e segredos empresariais valem duas vezes mais que dados de custódia, os quais se referem a informações de cartões de pagamento e dados médicos e de clientes.

"Os segredos compreendem dois terços do valor dos portfólios de informação das empresas. Apesar dos mandatos judiciais crescentes enfrentados pelas empresas, os ativos de dados de custódia não são os mais valiosos nos portfólios de informação das empresas. Conhecimentos proprietários e segredos empresariais, por outro lado, são duas vezes mais valiosos que os dados de custódia. Como ilustram os recentes ataques a empresas, os segredos são alvos de roubo.[3]"

Apesar do fato de que quase nove dentre dez empresas que armazenam dados confidenciais no exterior realizam

uma análise de risco formal, um aumento em relação a 2008, as empresas ainda armazenam dados em países de alto risco. Embora seja difícil rastrear os ataques até um país específico, China, Rússia e Paquistão são percebidos como os menos seguros para o armazenamento de dados. Estes são os mesmos três países que foram considerados os menos seguros em 2008. Os países considerados mais seguros em 2008 foram Reino Unido, Alemanha e Estados Unidos, e isso permanece em 2010.

Figura 1. A sua empresa evitou fazer negócios com esses países?



"De fato, as políticas não são aferidas frequentemente por seus gestores, o que abre várias janelas de oportunidade para a realização de atos ilícitos."

Comissão de Crimes de Alta Tecnologia da OAB – SP

Muitas empresas não avaliam ameaças e riscos tão frequentemente quanto deveriam. Mais de um quarto das empresas avaliam apenas duas vezes por ano ou menos as ameaças ou riscos aos quais seus dados estão expostos. Mais da metade das empresas determina por conta própria a frequência dessas avaliações de risco, em vez de seguir recomendações de auditores ou requisitos regulatórios.

Como disse a Comissão de Crimes de Alta Tecnologia da OAB – SP: "A grande maioria das empresas de vários setores não dispõe de controle sobre suas políticas de segurança da informação e nem mesmo possui grupos de diversas áreas corporativas voltadas para discutir esses eventos. De fato, as políticas não são aferidas frequentemente por seus gestores, o que abre várias janelas de oportunidade para a realização de atos ilícitos. A impressão é de que não há punições para tais atos corporativos. A empresa precisa trabalhar a mudança dessa imagem com treinamentos constantes voltados para a proteção do capital intelectual."

Na China, Japão, Reino Unido e Estados Unidos, as empresas gastam, em média, mais de US$ 1 milhão por dia em sua TI. Nos Estados Unidos, China e Índia, as empresas gastam, em média, mais de US$ 1 milhão por semana na proteção de informações confidenciais no exterior.

Mais de um quarto das empresas avaliam apenas duas vezes por ano ou menos as ameaças ou riscos aos quais seus dados estão expostos.

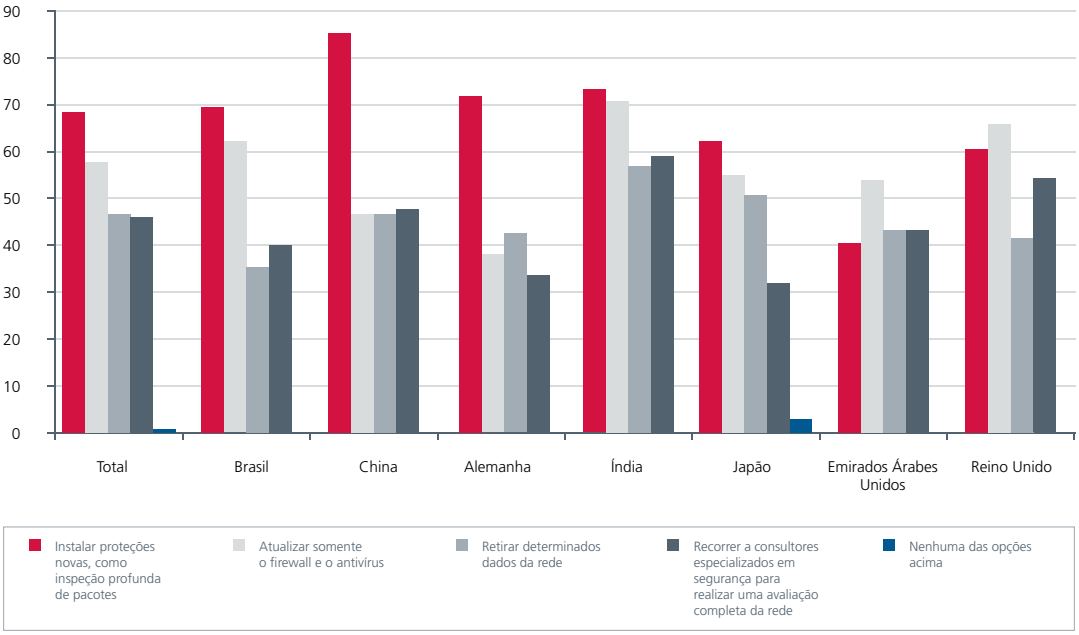
Na China, Japão, Reino Unido e Estados Unidos, as empresas gastam, em média, mais de US$ 1 milhão por dia em sua TI.

Aproximadamente metade das empresas pesquisadas está procurando aumentar seus gastos de segurança de TI em atualizações de hardware, atualizações de software, hospedagem externa de dados e outros serviços. Aproximadamente metade das empresas preveem que seus investimentos na proteção de informações confidenciais aumentarão, com apenas uma dentre 20 procurando reduzir seus gastos.

Apesar do crescimento nos gastos de segurança de TI, as soluções costumam ser reativas. Quando providências são tomadas, as empresas têm maiores probabilidades de instalar uma proteção nova, como inspeção profunda de pacotes, conforme relatado por mais de dois terços dos entrevistados. O método mais popular de proteção de dados confidenciais é através do uso de software antivírus, firewalls e sistemas de prevenção/detecção de intrusões (IDS/IPS), implementados por mais de quatro dentre cinco empresas.

É digno de nota que quase metade dos entrevistados disse que "retirariam determinados dados da rede" para protegê-los contra vazamentos. Aqui, a segurança dos dados é considerada como sendo mais importante para a empresa do que a disponibilidade ou utilização dos dados.

Figura 2. Quais medidas estão sendo tomadas para corrigir e proteger os sistemas para o futuro?



A proteção de dispositivos móveis continua a representar um desafio para as empresas, sendo que 62% dos entrevistados identificam isso como um desafio. O maior desafio que as empresas enfrentam ao gerenciar a segurança da informação é a natureza mutável dos ataques, seguida muito de perto pela proliferação de dispositivos e serviços, como mídias removíveis, telefones inteligentes e redes sociais. A mobilidade continua a dar poder e a permitir que as forças de trabalho realizem mais do que nunca, e essa tendência não para de aumentar. Simultaneamente, os canais de mídia social são de interesse crescente para as empresas aproveitarem. Essas duas forças representam um aumento astronômico no nível de risco que as empresas enfrentam em relação a dados vazados. Isso, aliado à necessidade das empresas de compartilhar dados críticos com parceiros-chave, significa que a abordagem tradicional à segurança cibernética precisa ser complementada. "Os telefones inteligentes muito provavelmente causarão um aumento nos esforços de pesquisa e desenvolvimento por parte dos criminosos devido à sua difusão e funcionalidade. Os serviços com base em nuvem também podem representar um novo alvo, não apenas para roubo de dados, mas também como infraestrutura barata ou recursos dentro de empreendimentos criminosos", afirma Marcel van den Berg, da Team Cymru.

A proteção de dispositivos móveis continua a representar um desafio para as empresas, sendo que 62% dos entrevistados identificam isso como um desafio.

Os serviços com base em nuvem também podem representar um novo alvo, não apenas para roubo de dados, mas também como infraestrutura barata ou recursos dentro de empreendimentos criminosos.

Seção 3: Ciberameaças e o impacto crescente sobre os negócios

A mídia tem mostrado um interesse crescente na perda de informações confidenciais, especialmente por parte de pessoas de dentro. Em 2008, três pessoas foram condenadas por roubar planos de marketing da Coca-Cola[4] e um ano depois, um ex-programador de computadores da Goldman Sachs foi preso por roubar código de computador utilizado para realizar transações proprietárias.[5]

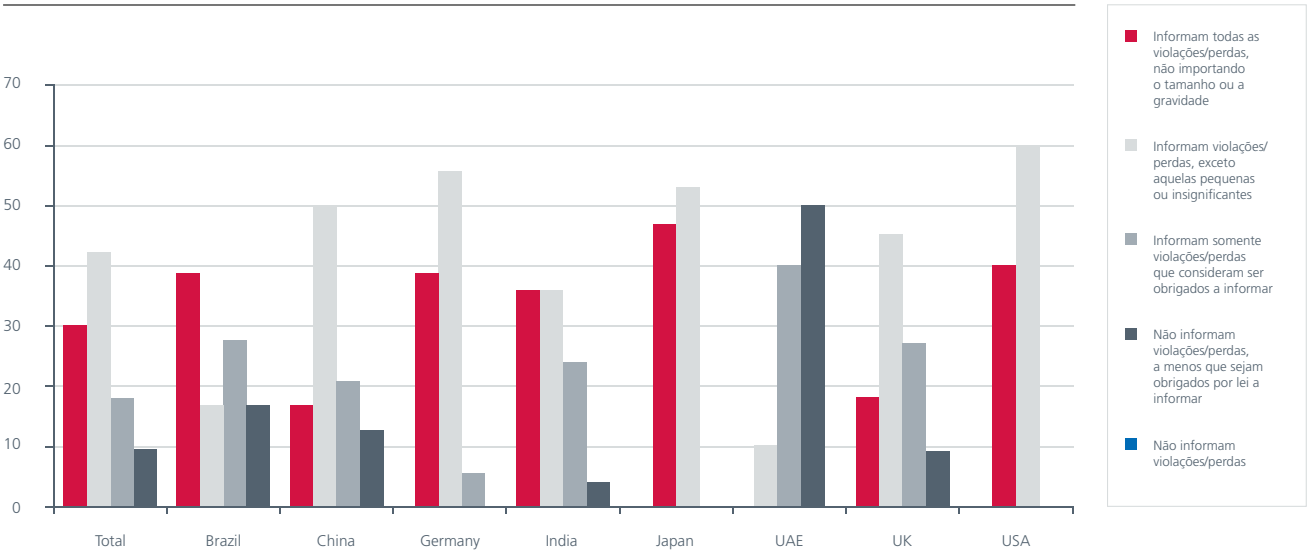
"Um único erro cometido por um funcionário incauto pode ter amargas consequências", disse Dinesh Pillai, CEO da Mahindra Special Services Group, uma empresa líder em consultoria de segurança corporativa da Índia. "Um funcionário sob influência de um atacante por meio de engenharia social pode resultar em vazamento de dados críticos, perdas financeiras e de reputação ou na interrupção do funcionamento da empresa. A maioria das tecnologias atuais utiliza algoritmos pré-carregados para detectar qualquer anormalidade. No entanto, o submundo é bem mais avançado em termos de capacidade tecnológica e engenhosidade, e pode identificar maneiras e meios de invadir os sistemas."

Além disso, de acordo com a Comissão de Crimes de Alta Tecnologia da OAB – SP, a ameaça originária de dentro costuma não ser meramente "acidental": "Com base em nossa avaliação, a maior ameaça interna são os profissionais considerados "intrusos" (intruders). Esses profissionais desempenham papéis de menor relevância para coletar informações e realizarem técnicas de engenharia social e cooptação de dados sensíveis."

"Muitas empresas não realizam um crivo mais aprofundado dos seus colaboradores diretos e indiretos. Em muitos casos há profissionais que são pressionados em suas comunidades carentes por facções criminosas. Estas facções solicitam ao funcionário que traga informações sensíveis como data de entrega de malotes, horários de abastecimento de postos eletrônicos, senhas de segurança interna e externa dentre outras informações da empresa em troca da segurança dos seus familiares."

Como resultado, tal como no estudo anterior, o impacto sobre a reputação é o que mais preocupa as empresas. Aproximadamente metade das empresas relatou isso como sua preocupação número um em relação a uma violação de dados envolvendo informações confidenciais ou propriedade intelectual. Hoje, uma empresa pública pode perder uma receita secreta, um plano de entrada no mercado ou outro segredo importante e hesitar em informar isso, devido à possível reação negativa dos clientes, dos acionistas e do mercado. A cobertura de mídia após uma violação de dados pode afetar a reputação da marca e o valor das ações. Por isso, os incidentes acabam não sendo divulgados.

Figura 3. Relatórios de violações de dados



Uma em cada sete empresas não informou violações e/ou perdas de dados para autoridades ou agências governamentais externas ou para acionistas. Somente três em cada dez empresas informam todas as violações/perdas de dados sofridas, enquanto uma em cada dez empresas informa somente as violações/perdas as quais é obrigada a informar, e nada mais. Atualmente, seis em cada dez empresas "escolhem" as violações/perdas que irão informar, dependendo de sua gravidade e potencial impacto.

A admissão de uma vulnerabilidade significa a possibilidade de atrair outros atacantes e, portanto, bem poucas empresas estão dispostas a vir a público comunicar perdas de capital intelectual.

Atividades de fusão e aquisição, parcerias e lançamentos de produtos são todas vítimas potenciais do roubo cibernético e dos malfeitores da economia clandestina. Aproximadamente um quarto das empresas teve alguma fusão ou aquisição ou o lançamento de um novo produto/solução interrompido ou atrasado por uma violação de dados ou pela ameaça provável de uma violação de dados. Quase metade de todas as empresas teve uma violação de dados pequena e quase um quarto das empresas sofreu uma violação de dados no ano passado, mais do que 2008.

As violações de dados também são caras. Em média, esses dados perdidos/violados custam às empresas mais de US$ 1,2 milhão, em comparação com menos de US$ 700.000 em 2008.

Talvez seja por isso que apenas um quarto das empresas realiza análises forenses de uma violação ou perda e que apenas metade tome providências para corrigir e proteger sistemas para o futuro, após uma violação ou tentativa de violação. Mais da metade das empresas decidiu, em um determinado momento, não investigar um incidente de segurança devido ao custo de tal investigação. As empresas são mais propensas a analisar e investigar pequenas violações de dados internamente, em vez de recorrer à ajuda externa. Essa falta de investigação significa que vetores de ataque potenciais não foram contidos e que invasões futuras são possíveis ou que a ameaça persiste. Os elementos internos não são identificados e as incongruências não são investigadas para identificar uma ameaça maior. Essa falta de correção pode sujeitar as empresas aos riscos de futuras violações.

A ameaça mais significativa relatada pelas empresas ao proteger suas informações confidenciais foi o vazamento de dados acidental ou intencional por funcionários. O cumprimento (ou a falta de cumprimento) dos procedimentos de segurança por parte dos funcionários é considerado o maior desafio para a segurança da informação das empresas. Isso foi avaliado como mais importante do que outros desafios, como múltiplos sistemas dentro da empresa ou a insegurança em sistemas de parceiros de cadeia de fornecimento. As políticas claramente não contiveram os vazamentos de dados, obrigando as empresas a optar por soluções técnicas robustas e inovadoras para reforçar suas diretrizes.

Uma em cada dez empresas informa somente as violações/perdas as quais é obrigada a informar, e nada mais.

Seção 4: Soluções e políticas andam de mãos dadas

Para muitas empresas, as decisões de gerenciamento de risco e segurança baseiam-se no rígido cumprimento de padrões de segurança, e não na proteção de seu capital intelectual. Essas empresas costumam não perceber que uma violação de dados pode ter um grande impacto sobre os negócios e a produtividade, retardando o desenvolvimento de produtos e interferindo com atividades de fusão e aquisição.

As políticas precisam estar lado a lado com soluções avançadas para fazer alguma diferença. Elas precisam ser implementadas em conjunto com tecnologias para inspeção profunda de pacotes, prevenção de perda de dados, monitoramento avançado de ameaças, análises forenses e até mesmo a retirada de determinados dados da rede.

Além disso, a distinção entre pessoas internas e aquelas externas é tênue. "Os atacantes sofisticados infiltram-se em uma rede, roubam credenciais válidas na rede e operam livremente – tal como alguém de dentro. Ter defesas estratégicas contra essas ameaças mistas internas é essencial e as empresas precisam de ferramentas contra ameaças internas que possam prever esses ataques de ameaça mista", disse Scott Aken, vice-presidente de operações cibernéticas da SAIC.

Tom Kellermann, vice-presidente de conscientização sobre segurança da Core Security Technologies, cita a falta de testes sólidos de penetração e cronogramas de correção como uma brecha nas estratégias de segurança cibernética de muitas empresas. Além disso, autenticação fraca, segurança sem fio permeável e tecnologia de detecção de intrusão em sistemas sem fio insuficiente contribuem para o problema.

Kellermann afirma que a resposta a incidentes e as capacidades forenses precisam ser avaliadas regularmente. "Especificamente, a ameaça avançada persistente ilustra a necessidade de uma resposta a incidentes que inclua o mapeamento de caminhos de ataque. Fornecedores externos de serviços gerenciados, como empresas de hospedagem e provedores de infraestrutura na nuvem, precisam ser obrigados contratualmente a testar sua postura de segurança e a cumprir com padrões mais elevados de segurança cibernética antes que se tornem "oásis no deserto" para predadores se infiltrarem", diz Kellermann.

"A maioria das empresas ainda está encarando a segurança cibernética como uma questão de perímetro. Com a contínua expansão do perímetro através de dispositivos móveis e computação na nuvem, o papel do departamento de segurança cibernética está se tornando mais difícil", acrescentou Aken.

Veja a seguir algumas tendências emergentes que estão mudando a maneira como as empresas definem ataques sofisticados e vazamentos internos:

Inspeção profunda de pacotes (DPI, Deep Packet Inspection) – Uma solução DPI atua como uma complementação altamente flexível da arquitetura de segurança existente, realizando análises completas de pacotes (camadas 2-7) em linha, quase em tempo real, de todos os pacotes (ou seja, sem perda de pacotes). Os aplicativos de software que residem sobre o hardware permitem que toda espécie de arranjo com base em regras remova dados dos pacotes que saem da rede, além de remover qualquer tipo de exploração do tráfego de entrada.

Segurança de rede com base no comportamento humano – Estas são soluções que ficam um passo à frente dos hackers ou infiltrados ao detectar as intenções através das atividades realizadas na rede. Essas soluções não utilizam assinaturas, anomalias ou heurística, mas comportamentos humanos que são comuns a todas as ações enganosas em uma rede que podem ser interrompidas antes de permitir que dados saiam da rede.

Ferramentas contra ameaças internas – Inovações recentes nas tecnologias contra ameaças internas criaram conjuntos de ferramentas que podem ser distribuídos em sistemas para monitorar de centenas a milhares de usuários internos simultaneamente, rastreando suas ações e identificando indícios inerentes às ações que podem ser motivo de alerta. Ao estabelecer perfis de atividades suspeitas na velocidade de transmissão, essas soluções podem interromper conexões caso os dados estejam sendo removidos de maneira inadequada ou se outras operações incomuns e críticas estiverem ocorrendo.

Análises forenses avançadas – Cada dispositivo digital, cada computador e cada telefone celular contam uma história que é rastreável através de uma trilha de "DNA digital" descoberta através de análises sofisticadas de computadores e redes. Serviços e ferramentas de software ajudam a descobrir e a extrair conteúdos críticos e a identificar comportamentos de usuários e identificadores únicos. Saber quais brechas e vulnerabilidades levou a um ataque é a primeira etapa na prevenção do próximo ataque.

Análise avançada de malware – Agora é possível descobrir malware de dia-zero que utilizará ou que está utilizando explorações de rede para atacar uma rede. Uma vez descoberto, o malware pode ser capturado para análise e resposta.

Conclusão

Embora as brechas de segurança cibernética não possam ser eliminadas completamente, as empresas podem reduzir bastante os riscos associados à saída de dados confidenciais de suas organizações. As empresas estão procurando uma maneira de monitorar o movimento de informações confidenciais e interromper a perda potencial de dados por intenção maliciosa ou por divulgação acidental. Tudo isso pode ser evitado.

Appliances podem ser instalados na rede para registrar e classificar tudo o que vai para a Internet, e há dispositivos que podem garimpar dados estruturados e desestruturados armazenados para que as empresas possam procurar e descobrir onde os dados confidenciais são mantidos. Embora esses dispositivos não sejam novidade, eles estão sendo continuamente aperfeiçoados e estão incorporando mais capacidades preditivas com base no comportamento humano. Soluções como inspeção profunda de pacotes, análise de comportamento humano e criptografia são todas soluções que crescerão em uso e eficácia nos próximos anos.

Atualmente, as empresas estão buscando mais do que uma conformidade de "preencher formulários" e procurando proteger seus dados mais confidenciais – como documentos de projetos, diagramas esquemáticos, planos de lançamento de produto, fórmulas farmacêuticas – ou seja, seu capital intelectual. Esses tipos de documentos são muito mais complexos que os números de documentos ou de cartões de crédito e exigem soluções de proteção avançadas.

Scott Aken acredita que a proteção da empresa começa com treinamento e a compreensão do que você está tentando proteger.

"A maioria das empresas gasta grandes quantias de dinheiro na proteção das partes menos críticas de sua rede, enquanto as" joias da coroa", ou seja, seu capital intelectual continua vulnerável. A análise abrangente do que reside na rede, combinada com uma estratégia sólida de defesa em profundidade e implementada por uma equipe devidamente treinada, pode fazer maravilhas pela proteção dos dados de uma empresa."

Colaboradores

Scott Aken, vice-presidente de operações cibernéticas da SAIC

Jenifer George, gerente do portfólio cibernético da SAIC

Marcel van den Berg, chefe de equipe de inteligência de negócios da Team Cymru

Simon Hunt, vice-presidente e executivo-chefe de tecnologia da Endpoint Security, McAfee

Tom Kellermann, vice-presidente de conscientização sobre segurança da Core Security Technologies

Dinesh Pillai, CEO do Mahindra Special Services Group

Erasmo Ribeiro Guimarães Junior, secretário e membro da Comissão de Crimes de Alta Tecnologia da OAB-SP, Brasil

Marco Aurélio Pinto Florêncio Filho, vice-presidente da Comissão de Crimes de Alta Tecnologia da OAB-SP, Brasil

Coriolano Aurélio de Almeida Camargo Santos, presidente da Comissão de Crimes de Alta Tecnologia da OAB-SP, Brasil

Referências:

1 *http://www.guardian.co.uk/world/2009/jul/22/germany-china-industrial-espionage*

2 *http://f1grandprix.motorionline.com/condannato-nigel-stepney-patteggia-1-anno-e-8-mesi/*

3 *http://www.rsa.com/products/DLP/ar/10844_5415_The_Value_of_Corporate_Secrets.pdf*

4 *http://www.justice.gov/usao/eousa/foia_reading_room/usab5705.pdf*

5 *http://www.bloomberg.com/apps/news?pid=newsarchive&sid=aSDxSdMlPTXU*

Sobre a McAfee

A McAfee, uma subsidiária pertencente à Intel Corporation (NASDAQ:INTC), é a maior empresa do mundo dedicada à tecnologia de segurança. A McAfee provê soluções proativas e com qualidade comprovada, além de serviços que ajudam a manter sistemas, redes e dispositivos móveis protegidos mundialmente, permitindo aos usuários conectarem-se à Internet, navegarem e realizarem compras pela Web com segurança. Apoiada pelo incomparável centro Global Threat Intelligence, a McAfee desenvolve produtos inovadores que capacitam os usuários domésticos, as empresas dos setores público e privado e os provedores de serviços, permitindo-lhes manter a conformidade com as regulamentações de mercado, proteger dados, prevenir interrupções, identificar vulnerabilidades e monitorar continuamente dados, além de incrementar a segurança em TI. A McAfee protege o seu mundo digital. O compromisso maior da McAfee é encontrar constantemente novas maneiras de manter nossos clientes seguros.

www.mcafee.com/br

Sobre a SAIC

A SAIC é uma empresa de aplicações científicas, tecnológicas e de engenharia listada na FORTUNE 500® que utiliza seu profundo conhecimento para resolver problemas de importância vital para o país e o mundo, em segurança nacional, energia e meio ambiente, infraestrutura crítica e saúde.

SAIC: From Science to Solutions® (da ciência às soluções). Para obter mais informações, visite www.saic.com

SAIC

McAfee

McAfee do Brasil Comércio
de Software Ltda.
Av. das Nações Unidas,
8.501 - 16° andar
CEP 05425-070,
São Paulo - SP, Brasil
www.mcafee.com/br