Dez previsões de segurança para 2012

O futuro está escondido no passado e muitas tendências que iniciaram ou ganharam força em 2011 irão se transformar em sérias ameaças em 2012. Como sempre, os criminosos cibernéticos vão farejar o dinheiro ao encontrar maneiras de conseguir dados valiosos de plataformas de computação emergentes. O smartphone de sistema operacional Android, do Google, será um alvo potencialmente lucrativo para os hackers, juntamente com as redes sociais e pequenas empresas. Enquanto o lucro é o incentivo principal para a maioria dos hackers, um número crescente está atento, alegando um caminho mais nobre ao justificar suas criminalidades como um mal necessário ao defenderem o que acreditam ser o correto. Espera-se que tanta moralidade direcione um aumento nos ataques politicamente motivados nos sistemas de controle industriais e em indústrias específicas.

A privacidade crescente gera serviços de geolocalização e altera o cenário em 2012, que será um ano memorável. A seguir as 10 tendências de segurança que prevemos.

10. Tecnologia emergente

Uma tendência em tecnologia que vai ganhar força em 2012 é o gerenciamento e análise de logs (registro) de hardware e software nas redes corporativas. Estes dados podem evidenciar malware, dando aos departamentos de TI uma chance de rapidamente neutralizar a ameaça. Subestimada no passado, a análise de log está sendo incluída nos produtos de fabricantes de segurança, uma vez que os clientes estão começando a entender como esta informação pode ser usada para impedir um ataque.

Os fabricantes especialistas neste campo incluem a Tripwire, LogLogic e Logrhythm, que a CRN intitulou de “Conhecimento necessário: fabricantes de segurança emergente”, em 2011. Direcionar a necessidade de segurança relacionada ao gerenciamento de log é a ascensão (o nascimento) nas ameaças avançadas e persistentes (advanced persistente threats – APT). Os ataques usando tais métodos visam empresas específicas com malwares sofisticados feitos para operar desapercebidos em sistemas infectados.

9. Geolocalização como destaque

A geolocalização está presente em todos smartphones, dando aos desenvolvedores de aplicativos a capacidade de rastrear usuários onde quer que vão. Por conta disto, a preocupação com privacidade irá manter a geolocalização no centro das atenções em 2012. Enquanto os consumidores aproveitam os serviços que os aplicativos de celulares fornecem ao elevar a tecnologia, algumas maçãs podres que conduzem clandestinos a rastrear ou a compartilhar dados podem provocar uma reação. Duas leis federais foram apresentadas no Congresso em 2011 para protegerem dados de geolocalização. Enquanto espera-se que nenhuma delas passe em 2012, as leis permanecerão na mídia. Ter privacidade dá margem para aumentar os esforços e forçar as empresas a adotarem um modelo opt-in ou um modelo de autorização do consumidor prévio para conseguirem informação sobre geolocalização.

8. Pequenas empresas são um alvo fácil

Ataques cibernéticos contra as pequenas empresas irão aumentar em 2012, pois os hackers buscam o caminho mais fácil para obterem lucro. As empresas em geral estão armazenando um crescente volume de dados valiosos e as pequenas empresas não são uma exceção. Entretanto, elas sofrem com a falta de reservas de dinheiro para segurança, comparada aos grandes players e desta forma tonam-se incapazes de construírem o mesmo nível de proteção, afirmam os especialistas. Fazer pequenas empresas especialmente vulneráveis é uma tendência graças ao fato de postergar ou deixar passar atualizações e substituições de sistemas antigos.

A expectativa é de vermos mais maneiras de ataques direcionados a pequenas empresas, desde engenharias sociais até injeções de SQL. A tendência não está esquecida pelos fabricantes. A Sophos tornou-se parceira da D&H Distributing em 2011, que possui uma rede

de canal e parceiros de mais de 25 mil revendas SMB. Para algumas pequenas empresas, a nuvem será um porto seguro. Esperem ver um número crescente de empresas contratando segurança gerenciada, deixando os fornecedores de serviço em nuvem se preocupar com as atualizações e manutenções.

7 . Leis aprimoradas

Algumas questões jurídicas graves serão relevantes em 2012, principalmente a norte-americana Norma de Segurança de Dados da Indústria de Cartões de Pagamento 2.0. A atualização inicia em 2012 e a maioria dos comerciantes não estão ainda muito preparados para lidar com isto, afirmam os observadores da indústria. Além disto, espera-se que a União Europeia restrinja sua Lei de Privacidade nas Comunicações Eletrônicas, que terá um grande impacto na privacidade de usuário da web. Mundialmente, os legisladores empurram as empresas para as conformidades com regulamentações ao aumentar as penalidades para brechas nos dados e por terem mais responsabilidades pelos dados dos consumidores.

Enquanto esta ação do governo pode melhorar algumas áreas de segurança, as empresas tendem a focar em conhecer o checklist de regulamentações dos legisladores, deixando passar alguns controles de segurança de tecnologia de informações básicas. Por exemplo, a maioria das regulamentações deixam passar uma grande escala de controle de melhores práticas, como um software de antivírus atualizado, segundo a empresa de consultoria de riscos Kroll. “Quanto mais brechas ocorrerem decorrentes de falhas de segurança, devemos esperar ver mais agências governamentais oferecerem guias específicos em avaliação de risco e controles de segurança padrões de TI“, disse Kroll. (Nota do IT Web: isso mostra uma tendência internacional, apesar de que cada país adota a legislação conforme sua necessidade)

6. Hacktivismo

Os lucros não serão o único motivo para os hackers em 2012. As questões políticas estão crescentemente por trás dos ataques e a tendência continuará. Este interesse se transformou no tão chamado hacktivismo em 2010 com a descoberta do worm Stuxnet que comprometeu sistemas de controle nas fábricas nucleares iranianas. O malware foi um alerta para o governos e corporações. Desde então, tem havido um aumento no número de anarquistas fracamente organizados. No ano passado, o LulzSec fez algumas manchetes entrando nos web sites dos governos federais e estaduais. Mais destes grupos de hacktivismo aparecerão em 2012 com muitos alegando estarem fazendo o bem. Por exemplo, o Anonymous, conhecido por defender o site de delação WikiLeaks, foram ameaçados, no ano passado, por membros do cartel de drogas mexicanos mascarados.

5. As ameaças industriais

As vulnerabilidades nos sistemas de controles industriais ficarão famosos em 2012, com grandes manipulações possíveis. Também chamado supervisão e aquisição de dados (SCADA), estes sistemas rodam em processos industriais, de infra-estrutura e fábricas, incluindo fabricação, rede elétrica distribuição e tratamento de água, oleodutos e gasodutos, sistemas de resfriamento e aquecimento nos aeroportos e em prédios comerciais e em muitos outros.

Os fabricantes vêm desenvolvendo interfaces de web para entrar nestes sistemas, dando aos hackers uma abertura em potencial. Além disto, os serviços de SCADA tem migrado para a nuvem, complicando a segurança ainda mais e aumentando as preocupações entre os especialistas. Desde 2010, quando o malware Stuxnet comprometeu as fábricas nucleares iranianas, a ameaça de um ataque na infraestrutura do país chamou muita atenção das autoridades de segurança do governo. A ascensão dos ataques com motivos políticos, ou hacktivismo será uma grande contribuição para a ascensão da ameaça.

4. As ameaças persistentes avançadas

Também conhecida como ataques com alvo, as ameaças persistentes avançadas se tornarão mais penetrantes em 2012. Estes ataques são menos arriscados e mais lucrativos do que

requisitar botnets que espalham spam e e-mail contendo malware, dizem os especialistas. Em decorrência disto, ataques em grande escala baseados em enganar quem recebe o e-mail clicando em um link ou abrindo um anexo estão diminuindo enquanto os APTs estão aumentando, informou a empresa de rede Cisco em seu relatório anual de segurança em 2011. Desde agosto de 2010, a quantidade de spam registrada pela Cisco caiu de 379 bilhões de mensagens por dia para 124 bilhões, o menor desde 2007. Ao contrário, os APTs estão crescendo.

Por exemplo, um homem na China foi responsável por um ataque cibernético contra pelo menos 48 empresas químicas e de defesa, relatou a empresa de segurança Symantec, em outubro. Dois outros ataques alvo foram relatados no ano passado: um contra cinco empresas multinacionais de petróleo e gás e outra contra 72 organizações incluindo a Nações Unidas, governos e corporações.

3. Os hackers serão mais sociáveis

Espera-se que ataques cibernéticos em redes sociais cresçam neste ano. Com mais do que 800 milhões de membros, o Facebook já foi alvo muitas vezes e espera-se que isto continue em 2012. Outra mídia social não ficará imune de ataques em perfis clonados e são utilizados como um canal para enganar os amigos e conhecidos na rede social ao clicar em um link malicioso. O Facebook foi o local no ano passado de alguns dos maiores ataques de perfis nas mídias sociais. Uma empresa de segurança dinamarquesa em novembro relatou o malware que usou uma foto enviada de uma conta clonada para pegar as pessoas com um click em um link que instalava um malware capaz de roubar senhas de bancos online. Felizmente, o tão chamado Zeus Trojan foi o primeiro descoberto em 2007, então as pessoas com o software de anti-virus atualizados estavam provavelmente protegidas.

2. Nuvens escuras

O número crescente de empresários e consumidores alcançando a nuvem tornou o software as a service popular. Com tantos dados pessoais e corporativos em servidores de prestadores de serviços, os criminosos cibernéticos vão torná-los um alvo prioritário em 2012, esperando encontrar vulnerabilidades em modelos de segurança que cresceram mais rapidamente do que o desenvolvimento dos padrões de nuvem.

“Se fossemos meteorologistas, definitivamente diríamos que temos um tempo nublado com grande possibilidade de tempestade,” a empresa de consultoria de risco Kroll disse em um recente comentário. Pesquisas recentes e relatórios mostram que as empresas estão subestimando a importância de não permitir que os prestadores de serviço fornecerem segurança. Em decorrência disto, brechas de dados na nuvem em 2012 irão evidenciar os problemas que os prestadores de serviço apresentam para os analistas forenses e respostas por incidentes. Enquanto isto, poderia ser considerado parte do processo de maturidade de uma nova tecnologia, as empresas devem estar bem mais atentas para evitar se tornarem vítimas de um incidente de um prestador de serviço.

1. Ameaça Android

Espera-se que os criminosos cibernéticos façam smartphones que rodam no sistema operacional Android, do Google, uma prioridade em 2012. Durante a última metade de 2011, a quantidade de malware feitas para o Android quádruplicou, uma vez que os hackers tentaram tirar vantagem da base de usuário que cresceu rapidamente e da abertura que o Google oferece além de incluíram a permissão de terceiros a distribuir aplicativos para o sistema operacional em qualquer web site. Este último significa que os criminosos podem lançar seus próprios sites para enganar as pessoas a baixarem softwares ilícitos.

Mesmo no Android Market oficial, os malwares disfarçados de jogos foram removidos do site e os especialistas culparam a falta de supervisão estrita para as brechas na segurança. O fabricante de segurança Kaspersky Lab disse que este ano pode marcar a aparição da primeira massa de worms para Android, capaz de espalhar via mensagem de texto e enviar links para a

loja virtual para distribuir malware. O fabricante também diz que o primeiro botnet móvel é mais provável no Android.

Fonte: It Web, 23 de mar 2012: [Portal]. Disponível em: < http://itweb.com.br>. Acesso em 23 de mar. 2012.