

2015 será lembrado como o ano da perda de dados. Quais ataques virtuais devem marcar o próximo ano? Pela primeira vez depois da fusão, os profissionais de segurança virtual da Raytheon|Websense compartilham suas previsões para o ano que vem. Os pesquisadores acreditam que devemos ficar atentos para: atividades ligadas às eleições presidenciais dos EUA; hackers roubando a carteira instalada em seu celular; e novas vulnerabilidades com o envelhecimento da Internet, entre outros problemas de segurança.

O ciclo das eleições norte-americanas deve contribuir para um aumento de ataques baseados no tema

Os hackers irão focar em campanhas, plataformas e candidatos políticos como oportunidade para desenvolver iscas usadas em ataques de engenharia social. Outros devem focar no hacktivismo, mirando candidatos e plataformas de mídia social. Além das ameaças mais previsíveis associadas a campanhas, plataformas e candidatos políticos, os hackers devem atacar a infraestrutura de todos os envolvidos no processo político (candidatos, sites de notícias e grupos de apoio). Os hacktivistas podem revelar informações pessoais ou usar contas comprometidas para distribuir informações falsas, aparentemente enviadas por algum candidato. O custo de falhas de segurança e defesas comprometidas será alto para aqueles que não seguem postura correta nessa época.

Carteiras móveis e novas tecnologias de pagamento apresentam oportunidades adicionais para o roubo e a fraude envolvendo cartões de crédito

Ataques contra dispositivos móveis e novas tecnologias de pagamento terão um impacto maior sobre a segurança de pagamento do que a EMV. O crescimento em meios de pagamento não tradicionais usando dispositivos móveis ou cartões inteligentes deve abrir portas para uma nova onda de ataques contra companhias de varejo.

A falta de manutenção da Internet deve aumentar custos e ser cada vez mais difícil de administrar

Como as conchas que aderem ao fundo do barco, o custo de manter a proteção na navegação deve começar a aumentar e causar enormes problemas no uso e segurança da Internet. Um número surpreendente dos sites mais populares da Internet não oferece o nível de segurança esperado em relação aos seus certificados. Problemas adicionais incluem: versões antigas e quebradas do javascript que representam uma porta aberta para os hackers; atualizações rápidas de sistemas operacionais e novas tendências nos processos do fim do ciclo de vida de software que causam problemas; e os novos aplicativos que são construídos usando código reciclado com vulnerabilidades antigas. Todos esses fantasmas do passado devem retornar para assombrar a internet em 2016.

A inclusão do sistema gTLD será uma nova oportunidade para hackers

O número de gTLDs a partir de novembro de 2015 ultrapassou 700 domínios, com outros 1.900 na lista. Conforme novos domínios de alto nível surjam serão rapidamente colonizados pelos hackers antes dos usuários legítimos. Aproveitando a confusão de domínios, os hackers criminais e governamentais devem criar ataques altamente sofisticados para infectar usuários com malware e roubo de dados.

Seguradoras de riscos virtuais devem criar um modelo atuarial de risco - mudando a definição e a implementação de sistemas de segurança

As companhias de seguro devem aprimorar seus produtos com qualificações, exceções e isenções que permitirão recusar pagamentos por ataques causados por deficiências de segurança. Os prêmios e reembolsos serão mais alinhados com a postura subjacente de segurança, ao lado de modelos mais avançados dos custos reais de um ataque. Além disso, as companhias de seguro

terão um grande impacto sobre os programas de segurança com a importância dos requisitos exigidos, chegando ao mesmo nível dos requisitos regulatórios (PCI, HIPAA, ISO 27001).

A Internet das Coisas (IOT) vem para ajudar - e atingir - a todos

As fronteiras entre dispositivos corporativos e pessoais estão desaparecendo, causando problemas e desafios de segurança que afetam a infraestrutura crítica. Os setores que utilizam um grande número de dispositivos conectados e sistemas em rede no dia a dia, como o setor de saúde, devem enfrentar um número ainda maior de vulnerabilidade e ameaças.

A adoção de DTP deve crescer dramaticamente entre companhias de outros setores

Com os ataques amplamente divulgados em 2015, a previsão de mudanças em seguros para o mundo virtual, a maior visibilidade cibernética nas reuniões executivas e a contínua preocupação com a perda de dados, haverá uma adoção mais agressiva de estratégias para a prevenção contra o roubo de informações fora do setor financeiro, o comprador tradicional dessas soluções. As equipes de segurança devem adotar a premissa que "já fomos atacados" para fortalecer sua capacidade de administrar o inevitável.

A sociedade terá uma visão mais madura da privacidade

O aumento na frequência das violações de dados, como visto em 2015, vem alterando a percepção sobre as informações pessoalmente identificáveis (PII). Outras violações e perda de PII irão conduzir grandes mudanças na maneira em que a privacidade é percebida. Assim como já aconteceu na década passada com o "direito de ser esquecido", prevemos que dentro dos próximos 10 anos grandes mudanças semelhantes em direitos de privacidade e expectativas irão surgir.

Fonte: [Risk Report](#), em 10.12.2015.