S21sec apresenta previsões sobre cibersegurança para 2017

bit.pt/s21sec-apresenta-previsoes-ciberseguranca-2017/

09/12/2016

O relatório de cibersegurança da S21sec acaba de ser publicado. No documento a empresa apresenta as suas principais previsões para 2017. Os ataques direcionados e as APTs (Ameaças Persistentes Avançadas) são apresentadas como as principais fontes de ameaças, e cujos alvos prioritários são o setor bancário e industrial.

Tendo em conta o relatório, o malware dirigido a dispositivos móveis vai aumentar de forma significativa, com maior destaque para o de tipo ransomware e em dispositivos Android. Os especialistas destacam ainda o facto de 2017 trazer mais de 150 novas famílias de ransomware. Para além disso, o impacto que o mercado vai sofrer com a figura do cibercriminoso autónomo a aumentar a sua prevalência contra o crescimento do cibercrime organizado também são destacados.

Os especialistas da S21sec destacam cinco grandes tendências em matéria de cibersegurança:

1. **O utilizador deixará de ser o principal alvo: vão crescer os ataques dirigidos contra grandes entidades**. O setor bancário receberá o maior número de APTs e o malware ATM será um dos principais vetores de ataque, como ficou patente nos recentes ataques reportados. Para além disso, os especialistas acreditam que estes serão responsáveis por provocar muitas das fugas de dados sensíveis deste setor. Também vai aumentar a exposição a ataques em dispositivos IoT.
2. **Os ciberataques serão especialmente direcionados a smartphones e vão aumentar os do tipo ransomware.** Desde 2015 que os especialistas têm vindo a observar um aumento destes ataques, que requerem uma menor elaboração relativamente a outros métodos de hacking. O alerta vai também para o possível aumento de Exploit Kits que permitem fazer trocas nos parâmetros do telemóvel para extorquir os proprietários ou o uso de recursos para proceder ao roubo de dados ou intercetar comunicações. Os ciberataques continuarão a afetar em maior escala o sistema Android do que o iOS. É importante também destacar que, em 2017, e perante o número de dispositivos conectados e a falta de segurança dos mesmos haverá um aumento de ataques do tipo DDoS.
3. **Crescerá o número de APTs e os tempos de infeção serão reduzidos no setor industrial.** Prevê-se um aumento dos ataques contra o setor industrial e continuaremos a ser alvo de atos de espionagem e sabotagem cibernética através de APTs cada vez mais sofisticadas. Observa-se também uma redução dos tempos de infeção nos sistemas, o que dificultará a tarefa de encontrar vestígios da sua presença. Para além disso, está previsto um aumento do número de ciberataques no setor da saúde devido à grande quantidade de dados de pagamento ou informação confidencial que é tratada, assim como pela multiplicidade de dispositivos conectados pouco seguros e expostos a malware neste setor.
4. **Aumentará a relevância do cibercriminoso autónomo.** Os grupos de cibercrime organizado vão continuar a atuar e com um papel importante no momento de concretizar com êxito os seus ataques. Contudo, esta necessidade de investimento inicial e de uma infraestrutura complexa vai dar lugar a um novo perfil de cibercriminoso autónomo. Para além de utilizar o método ransomware, os especialistas apostam também num aumento do Malvertising-as-a-Service, com o qual serão capazes de obter benefícios económicos sem ataques de grande preparação.
5. **Apesar da crescente consciencialização, muitas empresas só vão avançar com medidas de segurança depois de terem sido atacadas em 2017.** Os especialistas da S21sec estão um pouco pessimistas em relação à consciencialização das empresas. Embora estejam a ser feitos esforços progressivos para aplicar medidas de segurança efetivas, a verdade é que muitas empresas prosseguem mantendo uma atitude reativa. Segundo os especialistas, é fundamental realizar um trabalho de consciencialização junto dos colaboradores das empresas sobre a sensibilidade da informação que gerem e as consequências que podem ter algumas das suas ações.

O mix das tecnologias **DBond e OSM** já é utilizado no programa de passaporte irlandês, proporcionando “o

maior nível de resistência à falsificação para aumentar a segurança do cartão e proteger a identidade dos cidadãos", refere a HID Global.

Os cartões OSM Multitech podem ser usados para aplicações que vão desde identidades nacionais e estrangeiras a benefícios de saúde, bem-estar, Seguro Social, licenças de motorista, permissões de armas e outras soluções para identificação segura.

"Os nossos cartões OSM estabeleceram o padrão para combinar a segurança visual, digital e física, ao mesmo tempo em que oferecem os mais altos níveis de durabilidade do cartão", disse **Rob Haslam**, vice-presidente e diretor administrativo da Government ID Solutions da HID Global. "Não temos histórico de um acontecimento que pudesse comprometer a segurança digital da tecnologia OSM e agora estamos a ajudar a alimentar o futuro de uma identificação cidadã mais segura", acrescenta o executivo.

O cartão Multitech OSM, DBond e outras tecnologias foram comprovados em vários programas nacionais de identificação de alto nível, incluindo o passaporte irlandês, bem como programas na Arábia Saudita, Angola e nos EUA. O cartão de Passaporte da Irlanda é o primeiro e único cartão de passaporte implementado na Europa para a passagem nas fronteiras e foi reconhecido pelo seu desenho inovador.

Além do lançamento, a HID Global destaca três novos aprimoramentos de segurança adicionados ao seu cartão e página de dados para passaportes. O recurso de segurança **eWindow** que utiliza uma personalização de laser para o desenho da antena, o recurso **UV Full Color Picture** que usa tintas coloridas UV para produzir imagens seguras que não podem ser vistas a olho nu, e o seu recurso de segurança **Clear Window** que permite imagens personalizadas para serem vistas de ambos os lados do cartão ou da página de dados.

A HID Global está também a apresentar a sua plataforma recém lançada HID goID, para IDs móveis que permite cartas de condução e outras formas de identificação emitidas pelo governo – como cartões de identificação de veículos, cartões de identidade, licenças especiais – para serem usados em **smartphones**, com segurança e sem comprometer a privacidade dos cidadãos.