Informação sobre ameaças e motivações de ataques informáticos.

Ameaças: Alvos de ataque e tipos de invasores

Quais são os objetivos dos invasores que tentam superar as medidas de segurança?

Os invasores geralmente se enquadram em quatro categorias:

1- Invasores não treinados (script kiddies) usam scripts finalizados da internet como um meio simples de atacar vulnerabilidades conhecidas “apenas porque conseguem”.

2- Invasores treinados (hackers) lançam ataques mais complexos com o objetivo de extorquir dinheiro de resgate de dados criptografados.

3- A espionagem industrial geralmente é praticada por invasores que usam seu conhecimento especializado para roubar dados ou prejudicar a empresa. Nesse caso, (ex-)colaboradores visam uma empresa específica.

4- Ataques orientados ao estado e a empresas são os mais perigosos. Esses ataques geralmente tiram proveito de vulnerabilidades previamente desconhecidas com vários objetivos em mente: acesso a dados confidenciais, manipulação de dados, interrupção de processos de fabricação ou até mesmo a paragem ou destruição de serviços com dados importantes para o funcionamento de uma empresa.

Além do ganho financeiro, a motivação também pode ser destabilizar um país – por exemplo, atacando o abastecimento de alimentos, interrupção dos serviços energéticos.

Ameaças

O Departamento Federal Alemão de Tecnologia da Informação, identificou como os dez ataques mais frequentes a instalações industriais/empresas:

1. Uso não autorizado de acesso de manutenção remota que possibilita o acesso externo a sistemas de controle industrial que muitas vezes não estão devidamente protegidos.

2. Ataques online por meio de Tecnologias de informação através de um departamento interno da empresa que está geralmente conectada à internet e que também pode estabelecer uma conexão com a rede Interna.

3. Ataques a componentes padrão, como sistemas operativos, servidores de aplicações ou bases de dados que normalmente contêm erros e vulnerabilidades que os invasores podem explorar. Esses componentes também podem ser implementados em sistemas ICS (sistemas de controle industrial), o que aumenta o risco.

4. Ataques DDoS (negação do serviço) em conexões de rede podem sobrecarregar os sistemas e interromper a funcionalidade da rede, colocam demasiada carga nos sistemas e com isso consegues parar servidores. Neste caso existe indisponibilidade do serviço.

5. O erro humano e a sabotagem através de invasores internos ou externos são uma grande ameaça. A negligência e o erro humano também ameaçam a confidencialidade e a disponibilidade.

6. O malware frequentemente é introduzido através de dispositivos de armazenamento removíveis ou componentes de TI (tecnologias de informação) móveis de colaboradores externos (exemplo: pen drives e portáteis pessoais infetados).

7. Os comandos de controle podem ser facilmente lidos e importados porque a maioria dos componentes de controle que comunicam através de protocolos de texto simples, o que significa que sua comunicação é desprotegida.

8. O acesso não autorizado aos componentes da rede é possível, se membros internos ou externos (estranhos) não autorizados, acederem a componentes (computadores) previamente ligados, usando métodos de autenticação inseguros que superaram as medidas de segurança.

9. Os invasores podem manipular os componentes da rede a fim de conduzir ataques do tipo man-in-the-middle ou facilitar o sniffing. Traduzindo estas duas expressões no primeiro caso o intruso está dentro da rede através de um software já instalado, o que facilita a sua ação consegue filtrar os dados dentro de uma rede, a segunda é idêntica, mas não filtra os dados os dados são todos enviados depois consegue ou não decifrar.

10. O potencial de falhas resultantes de influências ambientais extremas ou defeitos técnicos nunca pode ser completamente eliminado, mas o risco e os danos emergentes podem ser minimizados usando os devidos componentes e medidas de segurança.

Departamento de Informática FMDUL

Novembro de 2021