Seguraça

Tiago Heinrich

UniSociesc Joinville

18/06/2020

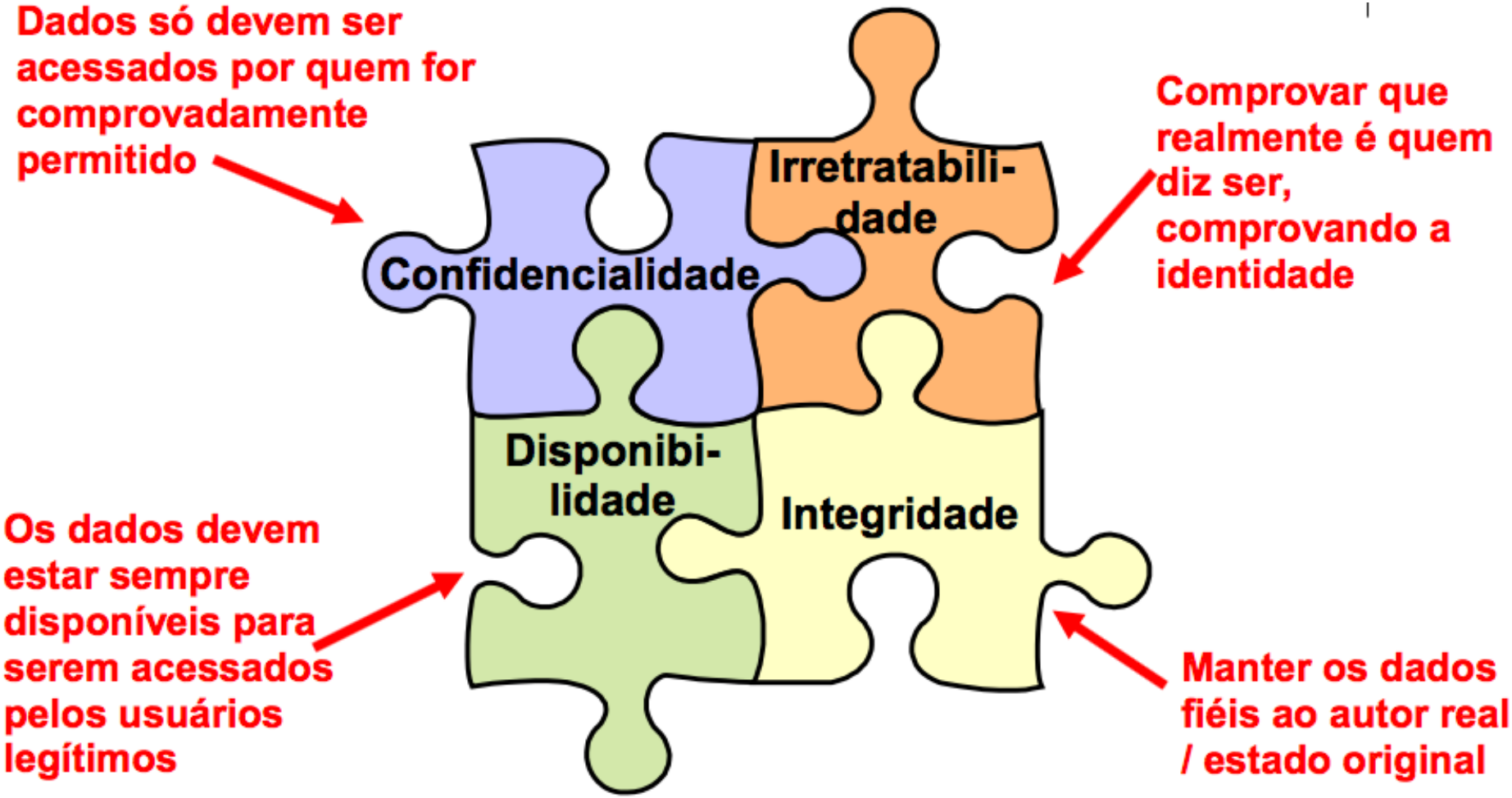
Contexto atual

- Ferramentas de trabalho indispensável em várias atividades
- Aumento de produtividade e qualidade das instituições relacionado diretamente ao uso de recursos tecnológicos providos por meios computacionais
  - Computadores, redes, tablets, smartphones, etc.
- Preocupação não apenas contra atacantes mas também com governos

Segurança para o Comércio Eletrônico

- Redes de computadores tornaram-se o meio fundamental para o funcionamento dos sistemas
- Recursos considerados importantes devem operar dentro de critérios definidos para obter os resultados pré-determinados
- Como manter as redes e as suas aplicações de modo que satisfaçam as necessidades dos provedores e clientes?
  - Aplicando a Segurança da Informação é possível obter a funcionalidade dentro de limites aceitáveis

Pilares da segurança



Objetivos

- Reduzir riscos
  - Sempre vai existir
  - Manter os riscos dentro dos limites aceitáveis
- Economizar dinheiro, através de ações pró-ativas
- Estabelecer planos para quando incidentes ocorrerem
- Assegurar-se / comprovar a real situação de segurança

Equação do Risco

- Possibilidade de um ativo sujeitar-se a fatores e incidentes que possam resultar em perdas ou danos, comprometendo a continuidade das atividades de uma organização
  - Ativo: algo tem que valor para uma organização
  - Fatores e Incidentes: vulnerabilidades ou ameaças
  - Perdas ou Danos: consequências
- Caso não exista a possibilidade de medir o risco, não existe a possibilidade de poder reduzi-lo

Vulnerabilidades?

- Falhas em software
- Falta de atualização (SO, aplicações, firmware, etc.)
- Erros de configuração
- Mal uso e erros humanos
- Serviços habilitados e não utilizados
- Políticas não aplicadas
- Falta de segurança física
- Falta de treinamento e conscientização
  - Senhas de acesso fracas
  - Armazenamento sem segurança
  - Falta de gerenciamento

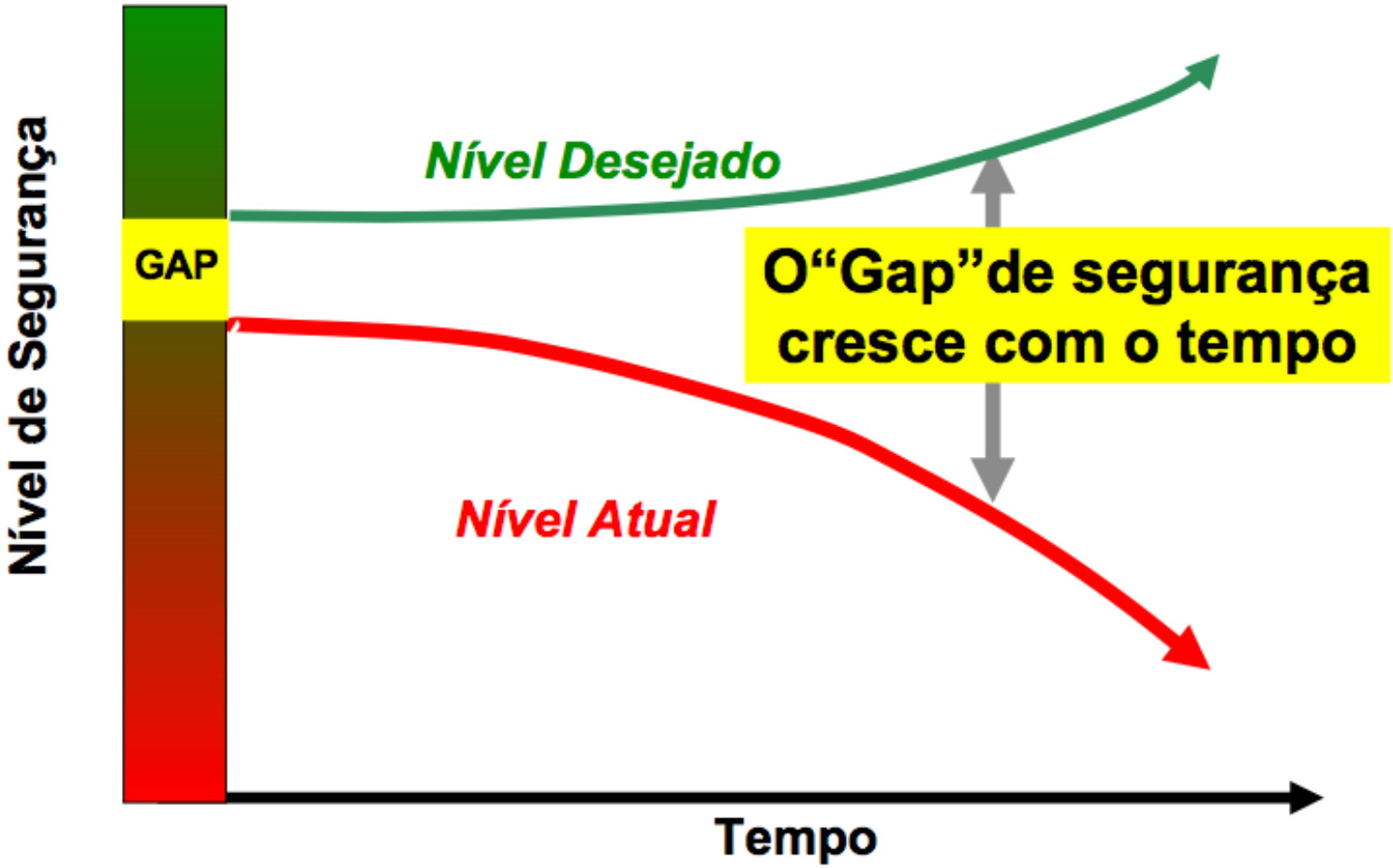
Esclarecendo?

- Hacker: alguém que possui profundo conhecimento sobre alguma área, possui iniciativa e é autodidata, busca sempre saber e aprender mais
- Cracker: um hacker que utiliza esse conhecimento em proveito próprio
- Lammer: alguém que está tentando adquirir conhecimento/experiência para tornar-se um hacker ou cracker
- Script-Kiddies: lammers que utilizam programas feitos por crackers para conseguirem/negarem acesso a sistemas
- Phreaker: um hacker de sistemas de telecomunicação

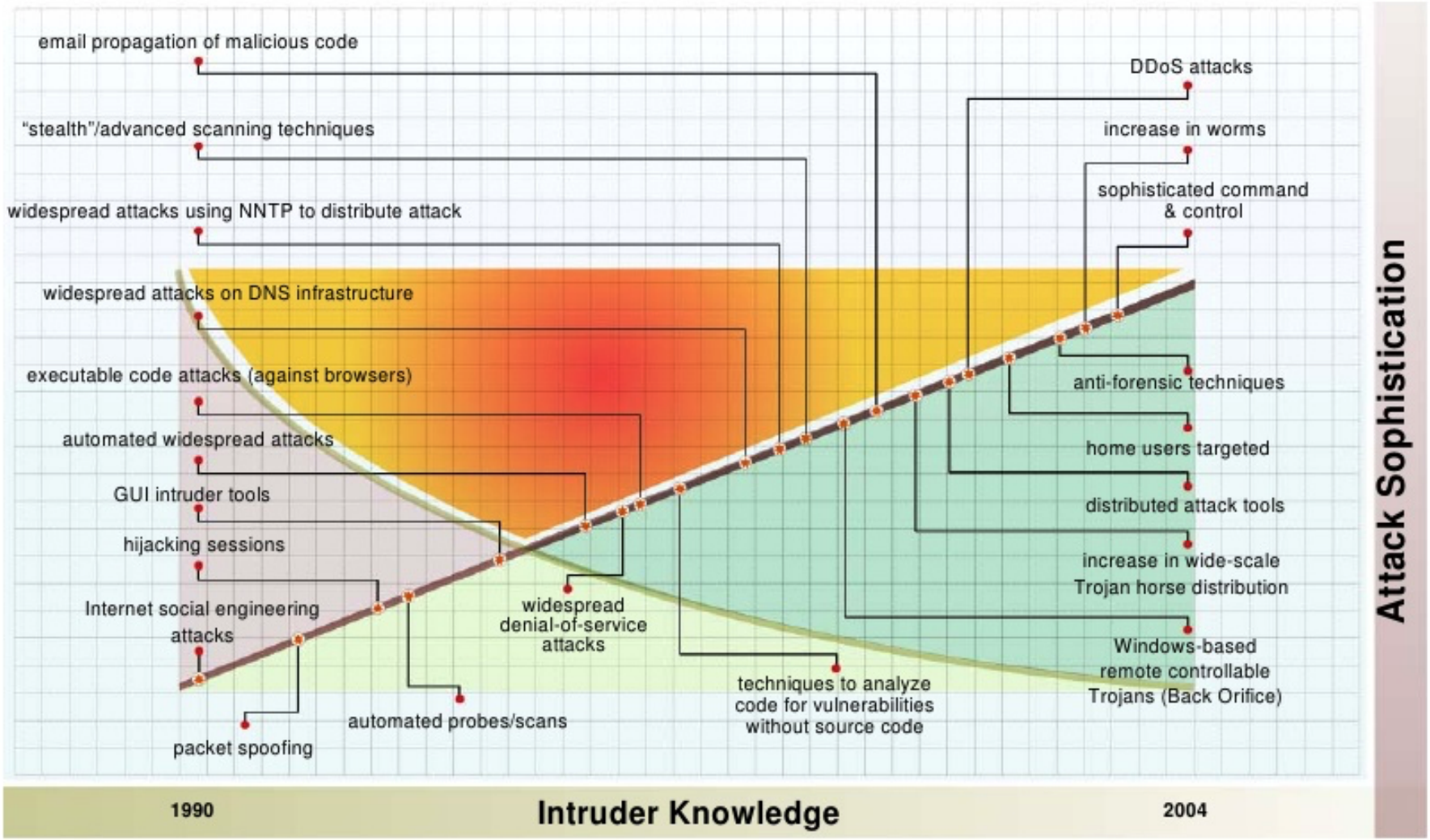
Vulnerabilidades?

- Abrir anexos de e-mails não solicitados
- Não instalar correções (patches) de segurança
- Instalação de software desconhecido (Software cracking ou sem certificados)
  - Microsoft office (background service) ou Jogos
- Atribuir a pessoas não treinadas para o gerenciamento da segurança
- Acreditar que o *firewall* faz milagre
  - Bloqueio ou filtragem de padrões definidos
- Configurações erradas de sistemas operacionais
- Utilizar sistemas de teste em produção

Security Gap



Attack sophistication vs. intruder technical knowledge



Como agem os atacantes?

- Os ataques podem ter finalidades diversas:
  - Sabotagem
  - Roubo de informações
  - Sabotagem e roubo de informações (raro, venda da informação pode perder o valor)
- Identificação de alvos
  - Varreduras, identificação de vulnerabilidades, remoção de dados e exfiltração de dados

Questões legais versus questões éticas

- Ética - ramo da filosofia que lida com o que se considera certo e errado
- Diretrizes que definam quais comportamentos são razoáveis sob determinado conjunto de circunstancias
- O que não é ético em uma cultura pode ser totalmente aceitável em outra
- Privacidade - o direito de não ser incomodado e de estar livre de intrusões pessoais despropositadas
- Duas regras tem sido seguidas em decisões judiciais:
  - O direito a privacidade não é absoluto; deve estar em equilíbrio com as necessidades da sociedade
  - O direito do público de saber é superior ao direito de privacidade do indivíduo

Cookies

- Cookie - pequena porção de dados trocada sucessivamente entre um site web e o navegador do usuários quando este navega pelo site; permite aos sites manter controle das atividades dos usuários sem pedir identificação
- Cookies podem ser usados para invadir a privacidade de uma pessoa
- Informações pessoais recolhidas por meio de cookies podem ser usadas de maneiras ilegais e antiéticas

Vulnerabilidades e ataques

- **Backdoor**
  - Qualquer método secreto de ignorar a autenticação normal ou os controles de segurança.
- **Denial-of-service attack**
  - Projetado para tornar uma máquina ou recurso de rede indisponível para os usuários pretendidos
  - DoS, DDoS, DRDoS ou Carpet bombing
- **Direct-access attacks**
  - Um usuário não autorizado que obtém acesso físico a um computador provavelmente pode copiar diretamente dados dele
  - worms, keyloggers, covert listening devices...
  - Dicas: Nunca compartilhe usuário

Vulnerabilidades e ataques

- **Eavesdropping**
  - Ato de ouvir clandestinamente uma "conversa"
  - MITM, grampo...
- **Multi-vector, polymorphic attacks**
  - Combina vários tipos de ataques e mudavam de forma para evitar controles de segurança cibernética à medida que se espalhavam
- **Phishing**
  - Adquirir informações confidenciais, como nomes de usuário, senhas e detalhes de cartão de crédito diretamente dos usuários, enganando-os
- **Privilege escalation**
  - Um invasor com algum nível de acesso restrito pode, sem autorização, elevar seus privilégios ou nível de acesso.

Vulnerabilidades e ataques

- **Social engineering**
  - Visa convencer um usuário a divulgar segredos, como senhas, números de cartões, etc., por exemplo, representando um banco, um contratado ou um cliente
- **Spoofing**
  - É o ato de se disfarçar como uma entidade válida por meio de falsificação de dados
- **Tampering**
  - Modificação maliciosa ou alteração de dados
  - Ex: certificado digital