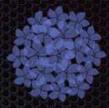
#include <std_disclaimer.h>

as opiniões e visões expressas nesta apresentação são estritamente as do autor e não reflectem necessariamente, muito menos comprometem, a Universidade do Porto

Jornadas Computação Científica 2019



PORTUGAL INCoDe.2030

‘confiança zero’

uma abordagem sistémica

António **Meireles** U.PORTO

‘confiança zero’

- modelo de segurança em Sistemas de Informação que exige uma verificação de identidade rigorosa para todas os utilizadores e dispositivos que tentem aceder a recursos numa qualquer rede, independentemente de estarem dentro ou fora do perímetro desta.
  - emerge como contraponto ao conceito tradicional de ‘perímetro’, ou seja o de *castelo* + muralha/fosso *vs* ‘mundo exterior’ o qual deixou não só, de fazer sentido como, pura e simplesmente, não é escalável.

- a conexão através de uma ‘rede’ específica deixa de determinar o tipo de serviços a que um utilizador pode aceder.
- o acesso a um qualquer serviço passa a ser determinado pelo que se sabe, no momento do acesso, quer sobre o utilizador, quer sobre o dispositivo que este está a usar.
- todos os acessos a serviços passam a ter que ser autenticados, autorizados e cifrados.

premissas-chave

- eliminação do uso de controlos baseados numa qualquer noção (estática) de perímetro (VPNs).
- simplificação e optimização da experiência final do utilizador.
- mais visibilidade na actividade dos utilizadores e maior facilidade na identificação de perfis de comportamento.
- muito menor TCO e muito maior ROI.

o conceito de '**utilizador**' redefinido

- está num estado 'activo' ?
  - pertence ao serviço X ?
    - os membros do serviço X precisam de aceder aos dados Y no sistema Z?
- o equipamento de onde está a ser feita a ligação está inventariado ?
  - os seus dados estão cifrados ?
    - o sistema operativo está actualizado?
      - e as aplicações?

o conceito de '**identidade**' redefinido

- **identidade** = **utilizador** + **equipamento** de **onde** acesso é efectuado, num **instante T**

tomada de decisões mais inteligente

- validações dinâmicas de confiança, em tempo real
  - o ERP da organização apenas pode ser acedido de equipamentos geridos centralmente.
  - o disco de um dispositivo para onde são feitos descargas de documentos com dados pessoais tem que estar cifrado.
  - a informação relativa ao 'papel' de qualquer colaborador pode ser acedida de qualquer dispositivo, autorizado, por qualquer outro colaborador da organização.

uma postura adequada de segurança

- quando as políticas de segurança são usáveis e coerentes, estas são mesmo utilizadas
  - equipamento mantido com *software* actualizado.
  - inventário actualizado de todo o equipamento em uso.
  - monitorização de todos os *endpoints* e recolha e análise de todo o tráfego.
  - comunicação apenas sobre canais cifrados.
  - autenticação de múltiplos factores.
  - eliminação do uso de credenciais estáticas.

'espinha dorsal'

- '**Identity Management**'
- '**Trust Inferer**'
  - um 'oráculo' que constantemente analisa os atributos e estado dos dispositivos para determinar o seu nível de confiança.
- '**Access Proxy**'
  - um '*reverse proxy*' colocado à frente de todo e qualquer recurso e que processa as solicitações ao mesmo.
- '**Device Inventory Service**'
  - um sistema que, de forma continua, recolhe e processa os atributos e estado de todos os dispositivos conhecidos.
- '**Access Policies Engine**'
  - uma representação programática dos recursos, níveis de confiança, e outras regras, que se querem respeitadas.
- '**Access Control Engine**'
  - um sistema central, o qual com base nas políticas definidas e dados disponíveis no momento, toma decisões de autorização em tempo real.

- nenhum dos componentes chave é ‘novo’ ou particularmente revolucionário.
  - alguns, muitos talvez, de uma forma ou outra já estão aliás em uso.
- ocorre é uma mudança fundamental de paradigma, onde se passa de uma *lógica* micro (táctica), em que a arquitectura resultante é um mero somatório das respostas a ‘problemas’, consoante estes vão surgindo, a uma arquitectura macro (estratégica), onde tudo, mesmo o inesperado, passa a obedecer a uma gramática comum, ortogonal e consistente entre si.

como chegar à ‘confiança zero’ numa organização?

1. saber *mesmo* do que a *casa* '*gasta*'

- realizar inventário exaustivo de todos os dispositivos em uso associados ao colaboradores - telefones móveis, estações de trabalho, laptops, tablets, etc.
- realizar inventário exaustivo de todos os activos a proteger - aplicações, BDs, servidores, serviços, etc.
- realizar inventário exaustivo de todos as credencias estáticas em uso - palavras-passe partilhadas, chaves ssh comuns, etc.
- visualizar a arquitectura/topologia em uso e recolher/analisar as interacções na mesma de modo a compreender o seu comportamento na prática
- recolher o estado de todos os dispositivos (cliente ou servidor)
  - o SO está actualizado ?
    - o disco cifrado ?

2. definir *o* quadro de *políticas* adequado - controlos & condições

- atributos de utilizador
- estado dos dispositivos
- regras baseadas na localização
- regras temporais
- grupos e perfis
- federação / associação de equipas
- regras específicas para determinados recursos

3. enumerar e descrever ‘histórias’

- narrativas para tarefas e processos, com vista a descrever os padrões, e respectivos anti-padrões, espectáveis nas rotinas diárias, tornando-os mais perceptíveis, e de forma a mostrar como estes devem influenciar a modelação das políticas - controlos e condições - a definir.
  - Ambrósia - equipa de desenvolvimento
    - quando uma nova versão do ERP interno à organização está disponível para testes, necessita de fazer ‘upload' da mesma para o respectivo servidor.
      - e se uma tentativa de ‘upload’, efectuada com as suas credenciais, surgir oriunda da Antártica ?
  - Tibúrcio - serviços financeiros
    - naturalmente no âmbito das suas funções tem acesso a muita informação, bancária, fiscal etc.
      - e se ocorrer uma tentativa de descarga de documentos com informação classificada, para um dispositivo, não actualizado, e sem, sequer, um disco cifrado ?

4. sobre o caminho

- nunca, jamais, tentar reinventar a roda e fazer tudo sozinho.
  - identificar o que é específico e o que são questões genéricas, comuns a qualquer organização do mesmo género.
    - sobre o que é genérico, identificar as boas práticas estabelecidas e segui-las.
- ser selectivo com o que se suporta, e o contexto em que se suporta:
  - sistemas operativos, protocolos, aplicações, etc.
- começar do 'geral' para o 'particular', refinando e iterando gradual e continuamente.
  - a ordem porque se implementa não é um detalhe - é crucial
- testar, automatizar, registar, comunicar, documentar
  - repetir as vezes que for necessário até que estes conceitos se tornem tão naturais como respirar.

5. ‘organização moderna’, *circa* 2020+

- **‘confiança zero’ = sustentabilidade + boa governação**


António Meireles
U.PORTO
Jornadas Computação Científica 2019
INCoDe.2030
ameireles@uporto.pt
obrigado!