UNIVERSIDADE PORTUCALENSE

Auditoria de segurança

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

O que é uma auditoria de segurança

- Baseada em politicas
- Avaliação do risco
- Examina as práticas e metodologias de um site
- Dinâmica
- Comunicação

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Que tipos de auditorias de segurança existem?

- Host
- Firewall
- Redes
- Redes de grande dimensão

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Políticas de segurança & documentação

- O que é uma política de segurança?
- Componentes
- Quem a deve escrever?
- Que tamanho deve ter
- Disseminação
- RFC 1244
- Outra documentação

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Componentes de uma política de segurança

- Quem pode utilizar os recursos
- Uso adequado dos recursos
- Concessão de acesso & de uso
- Privilégios de administrador do sistema
- Direitos e responsabilidades do utilizador
- O que fazer com a informação sensível
- Configurações de segurança desejadas dos sistemas

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

RFC 1244
``Site Security Handbook''

- Define políticas de segurança & procedimentos
- Violações da política
- Interpretação
- Divulgação
- Identificação de problemas
- Resposta a incidentes
- Atualizações

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Outra documentação

- Inventário de Hardware e software
- Topologia da rede de dados
- Pessoas chave
- Números de emergência
- Registos do incidente

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Por que fazer uma auditoria de segurança?

- Informação é poder
- Expetativas
- Medir a conformidade com as politicas
- Avaliar os riscos e nível de segurança
- Avaliação dos danos potenciais
- Gestão de alterações
- Resposta a incidentes de segurança

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Quando efetuar uma auditoria?

- Emergências!
- Antes do horário nobre
- Manutenção programada

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Como fazer uma auditoria de segurança

- Antes da auditoria: Verificar as ferramentas e o ambiente
- Auditoria/revisão da política de segurança
- Recolha informações de auditoria
- Gerar um relatório de auditoria
- Tomar ações com base nas conclusões do relatório
- Guardar a informação e o relatório

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Verifique as ferramentas e o ambiente

- A regra de ouro da auditoria
- Problema de inicialização
- Ferramentas de auditoria
- A plataforma de auditoria

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

A regra de ouro da auditoria

- Verifique se todas as ferramentas utilizadas para a auditoria não foram “alteradas”.
- Se os resultados das ferramentas de auditoria não podem ser confiáveis, a auditoria é inútil

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

O problema de inicialização

- Se a única maneira de verificar que as ferramentas de auditoria estão ok é utilizar ferramentas de auditoria, então...

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Confiança nas ferramentas de auditoria

- Escritas pelo utilizador
- Encontre uma fonte fidedigna
- Verificada através da assinatura digital (MD5)

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Principais ferramentas de auditoria

- SAINT/SATAN/ISS
- Nessus
- lsof /pff
- Nmap, tcpdump, ipsend
- MD5/DES/PGP
- COPS/Tiger
- Crack

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

A plataforma de auditoria

- Deve ter segurança extraordinária
- Deve ser necessário acesso físico para a utilizar
- Não estarem a correr serviços de rede

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Escolher uma plataforma de auditoria de segurança: Hardware

- Computador portátil
- Ethernet (Tantas ligações quantas as possíveis)

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Escolher uma plataforma de auditoria de segurança: Software

- Unix / Linux
- Ferramentas de auditoria
- Ferramentas de desenvolvimento

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Auditoria/revisão de política de segurança

- Utilizar uma existente ou uma “padrão”
- Tratar a política como uma ameaça potencial
- Tem todos os componentes básicos?
- As configurações de segurança são abrangentes?
- Examinar os procedimentos de divulgação

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Política de segurança

- Trate a política como uma ameaça potencial
- Políticas más são piores do que nenhumas
- Boas políticas são muito raras
- Verifique a clareza e integralidade
- Gramática pobre e ortografia não são toleradas

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Tem todos os componentes básicos

- Quem pode utilizar os recursos
- Uso adequado dos recursos
- Concessão de acesso e utilização
- Privilégios de administrador do sistema
- Direitos e responsabilidades dos utilizadores
- O que fazer com as informações confidenciais

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

São as configurações de segurança exaustivas?

- Os detalhes são importantes
- Contempla problemas técnicos específicos
- Permissões de confiança devem ser claramente indicadas
- Indica ferramentas especificas que devem ser utilizadas
- A calendarização de segurança deve ser indicada
- Os ficheiros de log devem ser regularmente examinados

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Examinar os procedimentos de divulgação

- As políticas são inúteis se não forem lidas e compreendidas pelos utilizadores
- O ideal é serem distribuídas em reuniões
- O email é útil para a divulgação das atualizações
- São necessários recibos de recebimento das politicas

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Recolha de informações de auditoria

- Entrevistas/conversas com utilizadores
- Revisão da documentação
- Investigação técnica

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Conversa/entrevista aos utilizadores

- Difícil de descrever, fácil de fazer
- Geralmente ignoradas
- Usuários, operadores, administradores de sistemas, zeladores, administradores ...
- Uso e padrões
- Têm visto / lido a política de segurança?

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Conversa/entrevista aos utilizadores (cont.)

- O que pode / não pode ser feito
- Poderem obter privilégios de administrador / sistema?
- Quais são os sistemas utilizados para?
- Quais são os sistemas críticos?
- Como vêm a auditoria de segurança?

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Revisão da documentação

- Inventário de Hardware e software
- Topologia de rede
- Pessoal chave
- Números de emergência
- Registos dos incidentes

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Investigação técnica

- Executar as ferramentas estáticas
- Verificação dos logs dos sistemas
- Validar os sistemas contra as vulnerabilidades conhecidas
- Validar os itens estáticos (ficheiros de configuração…)
- Verificação da existência de programas que são executados com maiores privilégios (SUID, SGID, …)

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Investigação técnica (cont.)

- Verifique a existência de serviços de rede extra (NFS, news, httpd, etc.)
- Verifique a existência de programas de “substituição” (wuftpd, TCP wrappers, etc.)
- Execute ferramentas dinâmicas (ps, netstat, lsof, etc.)
- Teste as defesas

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Executar as ferramentas estáticas

- Nmap
- SAINT/SATAN/ISS
- Crack
- Nessus
- COPS/Tiger

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Siga execução de inicialização

- Boot (P)ROMS
- init
- Programas executados no arranque

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Verificar os itens estáticos

- Examine todos os ficheiros de configuração dos processos em execução (inetd.conf, sendmail.cf, etc.)
- Examine os ficheiros de configuração de programas que podem iniciar-se dinamicamente (ftpd, etc.)

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Procure por programas privilegiados

- Procure todos os programas SUID/SGID
- Verifique todos os programas que são executados como root/Administrador
- Examinar também:
  - Ambiente
  - Caminhos de execução (Paths)
  - Ficheiros de configuração

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Valide todas as “confianças”

- rhosts, hosts.equiv
- NFS, NIS
- DNS
- Sistemas de janelas

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Verificar a existência de serviços extra de rede

- NFS/AFS/RFS
- NIS
- News
- WWW/httpd
- Proxy (telnet, ftp, etc.)
- Autenticação (Kerberos, security tokens, serviços especiais)
- Protocolos de gestão (SNMP, etc.)

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Validar a existência de programas de substituição

- wuftpd
- TCP wrappers
- Logdaemon
- Xinetd
- GNU fingerd

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Guardar resultados e relatórios

- Guardar a informação para a próxima auditoria
- Não guarde a informação online
- Usar criptografia forte se a informação for armazenada eletronicamente
- Limite a distribuição da informação para aqueles que a "necessitam de a conhecer"
- Imprima o relatório, assine-o e numere as cópias

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA