Segurança Informática

Aula 9

Programa

1. Conceitos introdutórios
2. Criptografia básica
3. Autenticação e Controlo de Acessos
4. Ameaças à segurança
5. Penetração em redes e sistemas
6. Políticas de segurança
7. Mecanismos de proteção e técnicas de defesa
8. Entidades de Segurança

8. Entidades de Segurança

Objetivos:

* Compreender a importância das entidades de segurança.

* Conhecer entidades de segurança a nível nacional e internacional.

Entidades de Segurança

- Num mundo altamente interligado e interdependente, a segurança e defesa do ciberespaço requer uma forte cooperação e colaboração entre aliados e parceiros, nacionais e internacionais.

- Responder aos desafios da segurança e defesa do ciberespaço requer uma abordagem em rede, pelo que a cooperação nacional e internacional nos diversos domínios de atuação é da maior importância.

Fonte: CNCS

Centro Nacional de Cibersegurança (CNCS)

- cncs.gov.pt

- O Centro Nacional de Cibersegurança atua como coordenador operacional e autoridade nacional especialista em matéria de cibersegurança junto das entidades do Estado, operadores de Infraestruturas críticas nacionais, operadores de serviços essenciais e prestadores de serviços digitais, garantindo que o ciberespaço é utilizado como espaço de liberdade, segurança e justiça, para proteção dos setores da sociedade que materializam a soberania nacional e o Estado de Direito Democrático.

Rede Nacional de CSIRT

- redecsirt.pt

- A Rede Nacional de CSIRTs (Centro de Resposta a Emergências de Segurança) é um fórum de excelência para a partilha de informação de carácter operacional. Tem como principais objetivos:
  - Estabelecer laços de confiança entre elementos responsáveis pela segurança informática de forma a criar um ambiente de cooperação e assistência mútua no tratamento de incidentes e na partilha de boas práticas de segurança;
  - Criar indicadores e informação estatística nacional sobre incidentes de segurança com vista à melhor identificação de contra-medidas pró-activas e reactivas;
  - Criar os instrumentos necessários à prevenção e resposta rápida num cenário de incidente de grande dimensão;
  - Promover uma cultura de segurança em Portugal.

CERT.PT

- O CERT.PT é um serviço integrante do CNCS que coordena a resposta a incidentes envolvendo entidades do Estado, operadores de serviços essenciais, operadores de Infraestruturas críticas nacionais e prestadores de serviços digitais.

- De forma geral, estamos a falar do ciberespaço nacional, incluindo qualquer dispositivo pertencente a uma rede ou bloco de endereçamento atribuído a um operador de comunicações eletrónicas, instituição, pessoa coletiva ou singular com sede em território Português, ou que esteja fisicamente localizado em território Português.

- O CERT.PT é membro da Rede Nacional de CSIRT e representante nacional na Rede Europeia de CSIRT, estabelecida pela Diretiva (EU) 2016/1148 (Diretiva SRI).

- O CERT.PT é membro acreditado do Trusted Introducer e Full Member do Forum of Incident Response and Security Teams (FIRST).

ECCE - Entidade Certificadora Comum do Estado

- ecce.gov.pt/

- A Entidade Certificadora Comum do Estado está credenciada pelo Gabinete Nacional de Segurança (GNS) como Certification Service Provider.

- A ECCE proporciona ao Governo, enquanto utilizador da Rede Informática do Governo (RInG), aos Órgãos de Soberania, enquanto utilizadores do Procedimento Legislativo, e a todas as Entidades e Organismos da Administração Direta ou Indireta do Estado, mecanismos de identificação eletrónica segura nas suas transações.

- Todos os serviços prestados pela ECCE, bem como os certificados emitidos por esta entidade, estão de acordo com a legislação atualmente em vigor relativamente a assinaturas eletrónicas, pelo que aqueles certificados gozam de total reconhecimento e aceitação. Os certificados emitidos pela ECCE permitem a assinatura eletrónica qualificada, ou seja, com força probatória legal, que é o mesmo que dizer equivalente à assinatura manuscrita.

Comissão Europeia

- ec.europa.eu/info/index_en

- Em 2013 a Comissão Europeia apresentou uma proposta de Diretiva relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União.
- A Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho foi aprovada em 6 de julho de 2016, e encontra-se atualmente em fase de transposição para os ordenamentos jurídicos internos dos países da UE.
- Os objetivos da Comissão Europeia em matéria de cibersegurança são:
  - Aumentar as capacidades de cibersegurança da UE e a cooperação neste domínio;
  - Reforçar o papel da UE na cibersegurança;
  - Desenvolver as políticas de cibersegurança dos países da UE de forma unificada.

ENISA - European Network and Information Security Agency

- enisa.europa.eu/

- A ENISA é uma agência de segurança das redes e dos sistemas de informação, dedicada ao desenvolvimento e implementação de medidas destinadas a garantir a segurança das redes e da informação na União Europeia (UE).

- A Agência presta apoio à UE e aos países da UE para a prevenção, deteção e resposta a incidentes de segurança da informação.

ISAC - Information Sharing and Analysis Center

- A ISAC é uma rede de cooperação entre grupos de interesse, transversal ao sector público e privado, que opera como uma plataforma assente em comunicações seguras, destinada à partilha de informações sobre cibersegurança, incluindo:
  - incidentes e vulnerabilidades,
  - troca de experiências,
  - partilha de informação relativa a políticas internas e outras práticas que contribuam para criar uma cultura de cibersegurança nacional.

NATO - North Atlantic Treaty Organization

- nato.int

- A NATO ou em português OTAN (Organização do Tratado Atlântico Norte) reconhece o ciberespaço como domínio de operações no qual poderá ser dada resposta a necessidades de defesa, tal como ocorre no ar, em terra e no mar.

- Os países aliados da NATO estão envolvidos na partilha de informação e assistência mútua na prevenção, mitigação e recuperação de ciberataques.

- A NATO promove também a sensibilização, formação e treino em ciberdefesa.

OSCE – Organization for Security and Co-operation in Europe

- osce.org

- A Organização para a Segurança e Cooperação na Europa adotou um conjunto de medidas tendentes a reduzir o risco de tensões entre Estados resultante do uso (ou mau uso) das Tecnologias de Informação e Comunicação.

- Este conjunto de medidas procuram complementar e reconhecer os esforços da comunidade internacional na promoção de uma cultura global de cibersegurança, e foram aprovadas pela decisão n.º 1202 do Conselho Permanente da OSCE, de 10 de março de 2016 (PC.DEC/1202), na forma de Confidence Building Measures (CBMs).

- As CBMs procuram promover a transparência e a estabilidade na cooperação inter-Estados. Encontram-se estruturadas em 16 medidas concretas que permitem aos Estados participantes identificar uma base comum e confiável de troca de informação entre si.

- O CNCS é o ponto de contacto nacional para as CBMs.

Projeto "No More Ransom"

- nomoreransom.org

- As agências de polícia e empresas de segurança informática juntaram forças para interromper as atividades criminosas com ligações ao ransomware.
- O website "No More Ransom" é uma iniciativa da Unidade de Crime de Alta Tecnologia da Polícia Holandesa, do European Cybercrime Centre (EC3) da Europol, Kaspersky e McAfee com o objetivo de ajudar as vítimas de ransomware a recuperar os seus ficheiros cifrados sem terem que pagar a criminosos.
- Uma vez que é muito mais fácil evitar a ameaça do que lutar contra ela assim que um sistema é infetado, o projeto também visa educar os utilizadores sobre como é que o ransomware funciona e quais as medidas que podem ser tomadas para uma prevenção efetiva.
- Quantos mais parceiros se juntarem ao projecto, melhores resultados poderão ser obtidos. Esta iniciativa é aberta a parceiros públicos e privados.

EUROPOL | EC3

- europol.europa.eu

- A Europol criou o Centro Europeu de Cibercriminalidade (EC3) em 2013 para reforçar a resposta da lei ao crime informático na UE e, assim, ajudar a proteger os cidadãos, empresas e governos europeus do crime on-line.

- Desde a sua criação, o EC3 fez uma contribuição significativa para a luta contra o cibercrime: esteve envolvido em dezenas de operações de alto nível, resultando em centenas de prisões e analisou centenas de milhares de ficheiros, a grande maioria dos quais provou ser maliciosa.

- Embora seja difícil fornecer estimativas confiáveis, alguns relatórios do setor sugerem que os custos globais do cibercrime estão na casa dos bilhões de euros por ano.

- Todos os anos, o EC3 publica a IOCTA (Internet Organized Threat Assessment - Avaliação de Ameaças ao Crime Organizado), o seu principal relatório estratégico sobre as principais descobertas e ameaças e desenvolvimentos emergentes em crimes digitais.

Organizações variadas

- **Associação Portuguesa para a Promoção da Segurança da Informação**
  - https://ap2si.org/
- **WiCyS - Women In Cybersecurity -** https://www.wicys.org/
- **CSA - Cloud Security Alliance -** https://cloudsecurityalliance.org/
- **CEGER -** https://www.ceger.gov.pt
- **ISC2 -** https://www.isc2.org
- **IASAP -** https://iasapgroup.org/
- **ISOC -** https://www.internetsociety.org/
- **ISOC-PT -** https://isoc.pt/

QUESTÕES

?