ACADEMIA DE CISCO

INTRODUCTION TO CYBERSECURITY AND CYBER SECURITY ESSENTIALS

(Cibersegurança e fundamentos à segurança cibernética)

OBJECTIVOS

Modulo 01

- Explicar o que é a cibersegurança;
- Compreender a importância de comportamentos seguros online;
- Descrever os diferentes tipos de software maligno e de ataques;
- Descrever as estratégias de proteção contra ataques utilizadas pelas organizações;
- Explicar que os profissionais de cibersegurança têm de ter as mesmas competências que os ciberatacantes, mas têm de trabalhar dentro dos limites da legislação local, nacional e internacional. E têm de utilizar as suas competências de forma ética;
- É objectivo deste curso também explicar a ciberguerra e o motivo pelo qual os países e os governos necessitam de profissionais de cibersegurança para ajudar a proteger os cidadãos e as infraestruturas.

Modulo 02

- Explicar a necessidade de cibersegurança;
- Descrever as características de criminosos e heróis no ambiente de segurança cibernética;
- Descrever os princípios de confidencialidade, integridade e disponibilidade, da forma que estão relacionados aos estados dos dados e a contramedidas de segurança cibernética;
- Descrever as táticas, técnicas e procedimentos usados por ciber-criminosos.;
- Explicar como os profissionais de segurança cibernética usam tecnologias, processos e procedimentos para defender todos os componentes da rede.
- Explicar a finalidade das leis relacionadas à segurança cibernética.

RECURSOS

Computador, Data show, Quadro e Servidor

DURAÇÃO

40 Horas

CUSTO

6.000,00 MT por participante individual

Pré - requisito

Conhecimentos de infraestrutura de redes físicas e lógicas

UNIDADE	INTRODUÇÃO À CIBERSEGURANÇA Modulo 01	DURAÇÃO
Definição de conceito, tipo de dados e piratas informáticos	O que é a Cibersegurança?; Identidade online e offline; **Dados pessoais como alvo**: credenciais online; dados de identidade; dados empresariais e governamentais; registos médicos, registos escolares. **Tipos de dados organizacionais**: Dados tradicionais e Internet of Things e Big Data.	40 horas
As consequências de uma falha de segurança	**Actividade de laboratório (de falha de segurança Nº 1)** **Actividade de laboratório (de falha de segurança Nº 2)**	
Questões jurídicas na cibersegurança	Questões legais pessoais; Questões legais empresariais e Lei e cibersegurança internacional	
Questões éticas na cibersegurança	Questões éticas pessoais e Questões éticas empresariais	
Definição de conceito	O que é a ciberguerra? A finalidade da ciberguerra e A necessidade de cibersegurança.	
Ataques, conceitos e técnicas	Como os profissionais de cibersegurança analisam o que aconteceu após um ciberataque e ciberataques modernos, considerados ataques mistos.	
Categorização de vulnerabilidades de segurança	Capacidade da memória intermédia excedida; Entrada não validada; Condições de corrida; Fraquezas em práticas de segurança e Problemas de controlo de acesso	

Vulnerabilidades de segurança	Vulnerabilidades de software e Vulnerabilidades de hardware	
Tipos de software maligno	Spyware, Adware, Bot, Ransomware, rootkit, Scareware, Virus, Trojan, Man-In-The-Middle (MitM) e Man-In-The-Mobile (MitMo); Os ataques de negação de serviço (Denial-of-Service, DoS) e Envenenamento SEO	
Sintomas de software maligno	Actividade de laboratório. (identificar tipos de software maligno); Actividade de laboratório. (exploração de vulnerabilidades) e Actividade de laboratório. (identificar o tipo de DoS)	
Proteger os dispositivos informáticos e Utilizar redes sem fios em segurança	Manter a firewall activo; Utilizar antivírus e antispyware; Gerir o sistema operativo e o browser; Proteger todos os seus dispositivos; SSID e a palavra-passe predefinidos para a interface administrativa; Cópia de segurança dos seus dados	
	Actividade de laboratório – (quem é o proprietário dos seus dados)	
Autenticação de dois factores	Um objecto físico e Um objecto físico	
	O Auth 2.0	
	Actividade de laboratório – (identificar a aplicação de segurança)	
Cisco Integrated Service Routers	Resultados de análise das portas Nmap	
	Aplicações de segurança.em: Routers, Firewalls, VPN, IPS, Software maligno/antivirus	
Boas práticas de segurança	Efetuar uma avaliação de risco; Criar uma política de segurança; Manter patches de segurança e atualizações e Estabelecer controlos de acess	

UNIDADE	CYBERSECURITY ESSENTIALS Modulo 02	
Domínios de segurança cibernética	**Google**: Um dos primeiros e mais poderosos domínios dentro do mundo cibernético, mais amplo da Internet. **O Facebook**: É outro domínio poderoso dentro da Internet mais popular. **O LinkedIn**: É ainda outro domínio de dados na Internet. **Novas tecnologias**: GIS (Geospatial Information Systems, Sistemas de informação geoespacial) e a IoT (Internet of Things).	**40 horas**
Criminosos virtuais	**Hackers**: Hackers "do bem" (white hacker), H. suspeitos (gray hacker) ou "H. do mal" (black hacker).	
Medidas para impedir criminosos virtuais	Criar bancos de dados de vulnerabilidade; Estabelecer sensores de aviso precoce e redes de alertas; Compartilhar informações de inteligência cibernética; Estabelecer padrões de gestão de segurança da informação entre organizações nacionais e internacionais. Como o padrão ISO 27000 e Promulgar novas leis para desencorajar violações de dados e ataques cibernéticos.	
Ameaças	**Ameaças comuns aos usuários finais**: registros pessoais, de educação, de emprego, de finanças, etc); **Ameaças a serviços de internet**: **(**Serviço de nome de domínio –DNS, Serviço de páginas Web, serviços de E-mail, etc) e Ameaças a sectores importantes de indústrias; **Ameaças ao estilo de vida das pessoas:** o direto à privacidade e o equilíbrio entre a segurança dos usuários da Internet.	

	AMEAÇAS INTERNAS Tratar erroneamente os dados confidenciais; Ameaçar as operações de servidores internos ou de dispositivos de infraestrutura de rede; Convidar acidentalmente malware para a rede por e-mail ou sites mal-intencionados. Cubo de segurança Cibernética fraquezas ou vulnerabilidades para obter acesso a recursos externos.	
Vulnerabilidades de dispositivos móveis	Monitoria e actualização de computadores para segurança de dispositivos móveis como iPhones, smartphones, tablets ou seja "traga seu próprio dispositivo (BYOD) é uma tendência crescente".	
Cubo de segurança Cibernética	Domínios de segurança cibernética; Confidencialidade, integridade e disponibilidade; Modelo de segurança cibernética **ISSO** e Decifração da palavra-passe de **Wi-Fi**	
A arte de garantir a integridade	Tipos de controles de integridade de dados usados, como algoritmos hash, salting e código de autenticação de mensagem de hash com chave (HMAC) e O uso de assinaturas digitais e certificados.	
Protecção de segredos	Criptografia, controle de acessos e ofuscação de dados.	