
CYBER
ACADEMY
FEBRABAN

MÓDULO 1

Fundamentos de Segurança Cibernética

O início da jornada tecnológica

Com a finalidade de automatizar o cálculo de tabelas balísticas, no ano de 1946 foi construído o primeiro computador digital, denominado ENIAC, que permitiu reconhecer a utilidade universal do invento e passou-se à construção de modelos com mais memória interna e que incorporavam o conceito de programa armazenado, fundamental para a utilização prática da máquina. Até os primeiros anos da década de 1950 várias máquinas foram construídas. Elas eram todas diferentes e todas artesanais, mas todas seguiam a chamada arquitetura von Neumann. Em meados da década de 1950, começou a produção dos primeiros computadores comercialmente disponíveis. A IBM saiu na frente neste processo o que lhe valeu o domínio quase absoluto do mercado de informática até meados da década de 1980.

No ano de 1957 a União Soviética lançou seu primeiro satélite espacial, o Sputnik. A contraofensiva a esse fato foi que o então presidente dos Estados Unidos John Kennedy prometeu enviar um americano para a Lua e criar um sistema de defesa à prova de destruição. Com essa última finalidade, e para acelerar o desenvolvimento tecnológico do país e coordenar atividades relacionadas com o espaço e satélites, foi criada a Agência de Investigação de Projetos Avançados (Advanced Research Project Agency – ARPA).

No ano seguinte a ARPA se enfraqueceu em razão da criação da National Aeronautics & Space Administration (NASA), com finalidade análoga, de um cargo no Departamento de Defesa com atribuições semelhantes, e pelo fato dos seus programas relacionados com mísseis balísticos terem sido direcionados a outros setores militares do governo. A saída para a ARPA foi modificar a perspectiva de pesquisa, incluindo novos projetos cujos resultados somente poderiam ser avaliados em longo prazo. Outro aspecto foi a realização de parcerias com instituições de ensino, de forma que tornou sua atuação mais técnica e científica. Em razão dessa mudança de foco, passaram a investir em assuntos que até então não eram adequadamente explorados, como a computação interativa e os sistemas de tempo compartilhado.

Em 1961 a UCLA - Universidade da Califórnia recebeu da Força Aérea o computador Q-32, da IBM, que auxiliou a inserção da informática no seio da ARPA. No ano seguinte, 1962, a Força Aérea, com a preocupação de proteger-se de uma eventual guerra ou ataque nuclear, solicitou à empresa Rand Corporation um estudo sobre uma rede de comunicação militar descentralizada, ou seja, despida de um núcleo central, que funcionasse mesmo que fossem destruídos alguns de seus terminais. A resposta foi um relatório que recomendava que o referido órgão militar solicitasse à American Telephone & Telegraph (AT&T) a implementação do projeto. A AT&T não concordou com o projeto e, inclusive, informou que implementar o projeto que envolvia a criação de uma rede digital de pacotes seria concorrer com ela mesma, que tinha uma rede analógica baseada em comutação de circuitos.

Levando em consideração a demanda, a resposta foi montar uma Rede de comunicações que não dependesse de um só núcleo central cuja destruição pudesse comprometer toda a Rede. O briefing era simples, mas complexo: desenhar uma Rede de comunicações totalmente independente que fosse invulnerável a qualquer tentativa de destruição ou controle por parte de qualquer entidade ou potência. A ARPANET foi acionada em 1969. Com o passar dos anos se consolidou a importância de criar uma rede capaz de integrar computadores que estivessem distantes e que por intermédio dela fosse permitida a comunicação de dados. Sob esse ponto de vista foi criada a ARPANET, inicialmente interligando a Universidade da Califórnia (Los Angeles e Santa Bárbara), a Universidade de Stanford (Santa Cruz) e a Universidade de Utah (Salt Lake City).

Os avanços só foram possíveis em razão dos estudos da época sobre a comutação por pacotes com a tese de doutorado de Leonard Kleinrock, professor da Universidade da Califórnia de Los Angeles (UCLA), em 1961 no MIT, análises de Paul Baran, da Rand Corporation, e projeto de redes de computadores, financiado pelo governo britânico, de Donald Davies, do Laboratório Nacional de Física do Reino Unido, no início dos anos 1960. A ARPANET passou a crescer continuamente. Para se ter uma ideia das proporções, havia 13 computadores na rede em janeiro de 1971, 23 em abril de 1972 e 38 em janeiro de 1973. Foi organizada a primeira demonstração pública da rede em 1972 por ocasião da “First International Conference of Computer Communications”, realizada no outono de 1972. Nesta oportunidade a rede já dava suporte a um amplo conjunto de serviços regulares, entre os quais estavam incluídos o login remoto e o correio eletrônico, cujo volume de uso surpreendeu os próprios responsáveis pela rede.

No ano de 1973 realizou-se a primeira conexão internacional da ARPANET, que interligou a Inglaterra e a Noruega. No final dessa década, a ARPANET substituiu seu protocolo de comutação de pacotes, denominado Network Control Protocol (NCP), para Transmission Control Protocol/Internet Protocol (TCP/IP). Em 1977 realizou-se uma demonstração do protocolo TCP/IP por intermédio da utilização de três redes: a ARPANET, a RPNET e a STATNET. Na década de 80 a ARPANET se disseminou pelos Estados Unidos e promoveu a interligação entre universidades, órgãos militares e governo. Foi implementado, no ano de 1986, a NSFNET – pela National Science

Foundation –, e a ARPANET começou a ser chamada de “Internet”. Para que ocorresse o grande salto na utilização da Internet houve estudos precursores de Ted Nelson, mas com Tim Berners-Lee e a rede WWW (World Wide Web) é que foram possíveis a expansão e a utilização comercial da Internet. Surgem os navegadores para facilitar a vida e utilização por usuários.

Assim, surge a Internet, a rede das redes, a rede mundial de computadores, tornando-se acessível a toda a população mundial, mesmo que com problemas de acesso e inclusão.

No Brasil o Instituto Brasileiro de Geografia e Estatística (IBGE) passou a utilizar um computador UNIVAC 1105 e, no ano de 1964, foi criado o Centro Eletrônico de Processamento de Dados do Estado do Paraná. Em 1965 foi criado o Serviço Federal de Processamento de Dados e o Brasil se associou ao consórcio internacional de telecomunicações por satélite (INTELSAT). Além disso, foi criada a Empresa Brasileira de Telecomunicações, vinculada ao Ministério das Comunicações, também recém-criado.

No ano de 1972 foi fabricado o primeiro computador brasileiro, denominado “patinho feio”, pela Universidade Federal de São Paulo (USP). Dois anos após foi criada a Computadores Brasileiros S.A. (COBRA) e em 1979 criou-se a Secretaria Especial de Informática. Outro passo importante para a consolidação da Internet no Brasil foi a conexão à Bitnet da Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP), do Laboratório Nacional de Computação Científica (LNCC) e da Universidade Federal do Rio de Janeiro (UFRJ), em 1988. A Secretaria Especial de Informática foi extinta em 1992, 13 anos depois de sua criação, e para suas atribuições foi criada a Secretaria de Política de Informática. Neste mesmo ano foi implementada a primeira rede conectada à Internet, que interligava as principais universidades brasileiras. Diferentemente da Internet que pode ser observada nos dias atuais, não existia interface gráfica. Os usuários conectados à rede conseguiam apenas trocar e-mails. Porém, no ano de 1995 passaram a disponibilizar o uso comercial da Internet no país. A velocidade máxima da conexão era de 9,6 Kbps. Neste mesmo ano ocorreu a criação do Comitê Gestor da Internet no Brasil (CGI.br), com a finalidade de “coordenar e integrar todas as iniciativas de serviços de Internet no país, promovendo a qualidade técnica, a inovação e a disseminação dos serviços ofertados”. Conforme dados do site Internet World Stats, em março de 2021 o Brasil contava com 74,8% de acesso da população brasileira à Internet.

O que é Segurança Cibernética?

Quando falamos sobre Segurança Cibernética, estamos nos referindo a todas as práticas, medidas e estratégias elaboradas para proteger um ativo digital que possui informações, sistemas computacionais, redes de dados, dispositivos de Internet das Coisas (IoT), que tem como objetivo garantir que esses ativos mantenham sua confidencialidade, integridade e disponibilidade.

Quando falamos de ativo digital, nos referimos às informações e recursos que possuem valor para você ou sua organização, e que pode incluir dados de informações de clientes, financeiros, de propriedade intelectual dentre outros. Todos estes ativos digitais são suscetíveis de ameaças, e a segurança cibernética tem como objetivo exatamente proteger esses ativos contra estas ameaças cibernéticas. Mas o que seriam essas ameaças cibernéticas?

Existem vários tipos de ameaças cibernéticas que podem incluir desde pessoas mal-intencionadas que possuem conhecimentos tecnológicos suficientes para comprometer sistemas, até programas maliciosos conhecidos como Malwares. No mundo tecnológico, ouvimos muito falar nos famosos Hackers que invadiram determinado sistema, ou que causaram determinado prejuízo por conta de um ataque cibernético, mas você sabia que existe uma grande diferença entre os termos Hacker e Cracker?
Em termos gerais, a palavra Hacker denota aquela pessoa que possui conhecimentos tecnológicos, que busca identificar falhas de segurança em sistemas e equipamentos tecnológicos, com o intuito de ajudar as empresas a resolverem as vulnerabilidades existentes, enquanto o Cracker é o "Hacker do mal", que rouba senhas, implementa malwares, compromete sistemas, ou de uma forma mais simplista: O Cracker comete crimes cibernéticos.

Independente do objetivo, seja ele auxiliar empresas ou cometer atos ilícitos, estes atores em geral utilizam-se de ameaças cibernéticas para obter sucesso em suas empreitadas.

Um tipo de ameaça bastante comum nos dias de hoje é o chamado Phishing, que tem como objetivo, tentar enganar as pessoas para obter informações confidenciais. Mas como e quando surgiram estas ameaças?

Juntamente com a evolução dos recursos tecnológicos, as ameaças praticadas via computadores foram se aprimorando com o passar do tempo. Para você ter uma ideia, a autorreplicação de programas de computador remonta ao final da década de 50, oriunda do matemático John Von Neumann. Tudo começou quando um grupo de programadores desenvolveu um jogo chamado Core Wars, capaz de se reproduzir cada vez que era executado, sobrecarregando a memória da máquina do outro jogador. Os inventores desse jogo também criaram o primeiro antivírus, batizado de Reeper, com capacidade de destruir as cópias geradas pelo Core Wars. A existência desse jogo, seus efeitos e a forma de desativá-lo, no entanto, vieram a público somente em 1983, por um artigo escrito por um de seus criadores, publicado em uma conceituada revista científica da época.

Já no ano de 1971, o Creeper Virus foi criado por um funcionário conhecido como Bob Thomas, de uma empresa que trabalhava com a construção da ARPANET, e consistiu em uma prova de conceito. Esse artefato malicioso apresentava a mensagem a seus usuários "I'm the creeper, catch me if you can!" e tinha capacidade autorreplicativa.

Em 1982, Richard Skrenta com apenas 15 anos de idade criou o Elk Cloner, considerado por alguns estudiosos do assunto o primeiro vírus desenvolvido para infectar computadores, apesar de, na época, o termo “vírus de computador” não ter ainda sido criado. Esse artefato contaminava o computador Apple DOS 3.3 e se difundia por cópias do disquete contaminado. É importante asseverar que esse código malicioso não causava grandes problemas, mas faria escola. Além de apresentar um pequeno ‘poema’ na tela do equipamento infectado, ele era capaz de gerar cópias de si mesmo quando um disquete era inserido no computador. Quando essa mídia era utilizada em outro sistema, o processo se propagava.

em 1984, Fred Cohen apresentou um paper, chamado “Experiments with Computer Viruses”, em que criou o termo “vírus de computador”, que denomina programas maliciosos, nocivos ao sistema como um todo. Dois irmãos paquistaneses, no ano de 1986, criaram um vírus de computador chamado Brain. Esse vírus atingia o setor de inicialização do disco4 e tinha como finalidade detectar uso não autorizado de um software médico de monitoramento cardíaco que haviam desenvolvido. Porém o código sofreu modificações maliciosas as quais o transformaram em um vírus que se espalhava através de disquetes infectados. O Brain causava lentidão nas operações do sistema e ocupava valiosos kilobytes de memória dos computadores.

Em relação ao assunto, porém, não existe uma posição pacífica sobre quando surgiu o primeiro vírus de computador, tendo em vista que, para alguns, o primeiro vírus foi o Elk Cloner e, para outros, o Brain. Cabe esclarecer que em 1986 também surgiram os primeiros cavalos de Troia de que se tem notícia. Exemplo disso é o caso do PC-Write: O PC-Write legítimo era um shareware de processamento de textos similar ao Word que temos hoje. O Trojan era uma suposta versão 2.72 deste software que havia sido lançada e, diferente do ANIMAL, tinha intuição maliciosa contra o sistema. Trabalhava em duas etapas ao ser executado: primeiro apagava a FAT (File Allocation Table) do sistema e então formatava o disco rígido do PC, deletando todos os dados.

O primeiro antivírus foi criado no ano de 1988 por Denny Yanuar Ramdhani em Bandung, Indonésia, e tinha a funcionalidade de imunizar o sistema do computador contra o vírus Brain. Segundo estudo elaborado pela Kaspersky, até 1995 os vírus de boot representavam aproximadamente 70% das ameaças, mas também existiam outros, como por exemplo aqueles que infectavam arquivos executáveis DOS.
Com a popularização de dispositivos utilizados para o acesso à rede mundial de computadores, também surgiram novos meios para a difusão de ameaças. No ano de 2004 surgiu o primeiro vírus de celular, oriundo das Filipinas. Denominado Cabir, a praga foi criada para infectar aparelhos que utilizavam o sistema operacional Symbian (hoje, presente em mais de 70% dos celulares). O objetivo do Cabir, que é disseminado por bluetooth, é descarregar toda a bateria dos celulares infectados. Em aparelhos contaminados pelo vírus, uma mensagem característica, com a palavra “Caribe” aparece no visor e se repete sempre que o equipamento é ligado.

Segundo Cintia Baio e Lilian Ferreira (2008), no mesmo ano o Cabir foi aprimorado por um brasileiro, que criou um vírus com código aberto chamado Lasco. Esse vírus foi criado por Marcos Velasco, hoje especialista em malware e dono de uma empresa de segurança, decidiu aprimorar o poder dos vírus para telefones móveis. Criou, então, o Lasco (também conhecido como Lasco A. ou Symbos_Vlasco.A), vírus de autoinstalação para Symbian, com código aberto e transmitido por bluetooth. A praga de Velasco também podia ser transmitida pelo computador e descarregava a bateria do celular. A evolução dos códigos maliciosos é constante e nos últimos cinco anos há uma predominância na utilização de sistemas maliciosos de coletas de dados pessoais e corporativos e, além disso, a criptografia de dados e informações (toda espécie de arquivos) constantes em bancos de dados e solicitação de sequestro em moeda virtual. Assim, surgem constantemente variantes de ransomware.

Agora que temos um pouco mais de contexto da história tecnológica apresentada até os dias de hoje, vamos abordar diretamente as principais ameaças e vulnerabilidades existentes.

Definições

Neste capítulo, provemos abaixo as definições dos principais conceitos utilizados, que sofreram uma padronização ao longo do tempo, graças ao resultado obtido da grande mudança entre a ISO 27001:2005 e a ISO 27001:2013. Os benefícios dessas mudanças são o alinhamento entre diferentes normas de gestão, as quais terão sempre o mesmo formato, e o uso das mesmas definições e dos mesmos conceitos. Dito isso, apresentamos abaixo a normalização de algumas definições:

- Ação preventiva – ação para eliminar a causa de uma potencial não conformidade ou outra potencial situação indesejável;
- Aceitação do risco – a decisão de aceitar um risco;
- Ameaça – causa potencial de um incidente indesejado, a qual pode resultar no dano a um sistema ou organização;
- Análise da informação – A análise da informação proporciona uma clara imagem de como uma organização manuseia a informação – como a informação “flui” pela organização.
- Análise de riscos – um processo para compreender a natureza do risco, a fim de determinar o seu nível. Uma análise de riscos proporciona a base para a estimativa do risco e para as decisões sobre o tratamento do risco. A análise de riscos inclui a estimativa do risco;
- Ataque – uma tentativa de destruir, expor, alterar, inutilizar, roubar ou obter acesso não autorizado a, ou fazer uso não autorizado de, um ativo;
- Autenticidade – propriedade de uma entidade ser o que afirma que é;
- Avaliação do risco – a avaliação do risco é o processo geral de identificação do risco, análise do risco e estimativa do risco;
- Confiabilidade – propriedade de consistência dos comportamentos e resultados

desejados;
• Confidencialidade – propriedade em que a informação não é disponibilizada ou divulgada para pessoas, entidades ou processos não autorizados. O conceito de confidencialidade busca prevenir a divulgação intencional ou não intencional do conteúdo de uma mensagem. A perda de confidencialidade pode ocorrer de diversas maneiras, tais como pela divulgação intencional de uma informação privada de uma empresa ou pelo mau uso das credenciais de acesso à rede;
• Controle – meios de gerenciar o risco, incluindo políticas, procedimentos, diretrizes e práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, gerencial ou legal, que modifiquem o risco à segurança da informação. É possível que os controles nem sempre exerçam os pretendidos ou assumidos efeitos de mudança, e o controle também é usado como sinônimo para salvaguarda ou contramedida;
• Diretriz – descrição que esclarece o que deve ser feito, e como, para alcançar os objetivos definidos nas políticas;
• Disponibilidade – propriedade de ser acessível e utilizável sob demanda por uma entidade autorizada. O texto formal anterior assegura o acesso confiável e em tempo oportuno a dados ou recursos de computação pelo pessoal apropriado. Em outras palavras, a disponibilidade garante que os sistemas estão ativos e funcionando quando necessário. Adicionalmente, este conceito garante que os serviços de segurança, que o profissional de segurança requer, estão em perfeito funcionamento;
• Estimativa do risco – é o processo de comparar os resultados de análise do risco com um critério de risco, a fim de determinar quando o risco e/ou sua magnitude é aceitável ou tolerável;
• Evento de segurança da informação – Ocorrência identificada de um estado de um sistema, serviço ou rede que indique uma possível violação da política de segurança da informação ou falha de proteção, ou uma situação previamente desconhecida que possa ser relevante em termos de segurança;
• Exposição – exposição é a circunstância de estar exposto aos prejuízos oriundos de um agente ameaçador;
• Gerenciamento de riscos – atividades coordenadas para direcionar e controlar uma organização no que diz respeito ao risco;
• Gestão da informação – a gestão da informação descreve os meios pelos quais uma organização eficientemente planeja, coleta, organiza, usa, controla, dissemina e descarta sua informação, e através da qual garante que o valor dessa informação é identificado e explorado em toda a sua extensão;
• Gestão de incidentes de segurança da informação – processo para detectar, reportar, avaliar, responder, lidar e aprender com os incidentes de segurança da informação;
• Gestão de segurança da informação – atividades coordenadas para dirigir e controlar uma organização no que se refere ao risco. O gerenciamento do risco tipicamente inclui a avaliação do risco, o tratamento do risco, a aceitação do risco e a comunicação do risco;

• Identificação do risco – é o processo de encontrar, reconhecer e descrever riscos. A identificação do risco envolve a identificação das suas fontes, eventos, causas e suas potenciais consequências. A identificação do risco também pode envolver dados históricos, análise teórica, opiniões, pareceres fundamentados e de especialistas, e necessidades das partes interessadas;
• Incidente de segurança da informação – um incidente de segurança da informação é indicado por um único ou uma série de eventos de segurança da informação, indesejáveis ou inesperados, que tenham uma probabilidade significativa de comprometer a operação dos negócios e ameacem a segurança da informação;
• Informação – informação é o dado que tem significado em algum contexto para quem o recebe. Quando informação é inserida e armazenada em um computador, ela é geralmente referida como dado. Após processamento, o dado de saída pode ser novamente percebido como informação;
• Instalações de processamento de informações – qualquer sistema de processamento de informações, serviço ou infraestrutura, ou os locais físicos que as abriguem;
• Integridade – propriedade de proteger a exatidão e a integridade dos ativos. O conceito de integridade assegura que sejam prevenidas modificações não autorizadas ao software e ao hardware, que não sejam feitas modificações não autorizadas aos dados, por pessoal autorizado ou não e/ou processo, e que o dado seja internamente e externamente consistente;
• Não repúdio – habilidade de provar a ocorrência de um suposto evento ou ação e suas entidades de origem;
• Política – a intenção e orientação geral formalmente expressa pela administração;
• Procedimento – forma específica de conduzir uma atividade ou processo;
• Processo – conjunto de atividades inter-relacionadas ou interativas que transformam entradas e saídas;
• Processo de gerenciamento de riscos – é a aplicação sistemática de políticas de gerenciamento, procedimentos e práticas às atividades de comunicar, consultar, estabelecer o contexto e identifica, analisar, avaliar, tratar, monitorar e revisar o risco. A ISO/IEC 27005:2011, que é a norma ISO para o gerenciamento do risco à segurança da informação, usa o termo “processo” para descrever todo o gerenciamento de riscos. Os elementos dentro do processo de gerenciamento de riscos são denominados “atividades”;
• Responsabilidade – atribuição de ações e decisões a uma entidade;
• Risco – efeito da incerteza sobre os objetivos. É a combinação da probabilidade de um evento e sua consequência. Um efeito é um desvio do que é esperado, o qual pode ser positivo e/ou negativo. Os objetivos podem ter diferentes aspectos (tais como financeiro, saúde e segurança, segurança da informação e metas ambientais) e podem ser aplicados em diferentes níveis (tais como estratégico, em toda a organização, projeto, produto e processo). Um risco é frequentemente caracterizado pela referência a potenciais eventos e consequências, ou uma combinação destes. O risco à segurança da informação é muitas vezes expresso em

termos de uma combinação entre as consequências de um evento de segurança da informação e a sua probabilidade de ocorrência. Incerteza é o estado, mesmo que parcial, de deficiência da informação relacionada a compreensão ou conhecimento de um evento, sua consequência ou probabilidade. O risco à segurança da informação está associado ao potencial de ameaças explorarem vulnerabilidades de um ativo de informação ou grupo de ativo de informações e, desse modo, causar danos a uma organização;

• Risco residual – risco que permanece após o tratamento do risco. O risco residual pode conter riscos não identificados e pode ser conhecido também como "risco retido";

• Segurança da informação – preservação da confidencialidade, integridade e disponibilidade da informação. Adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, também podem ser incluídas;

• Sistema de gerenciamento da segurança da informação – SGSI – parte do sistema total de gerenciamento, baseado em uma abordagem de riscos de negócio, para estabelecer, implementar, operar, monitorar, revisar, manter e melhorar a segurança da informação. O sistema de gerenciamento inclui estrutura organizacional, políticas, atividades de planejamento, responsabilidades, práticas, procedimentos, processos e recursos;

• Sistema de informação – aplicação, serviço, recursos de tecnologia da informação ou qualquer outro componente de manejo da informação. Em um sentido bem amplo, o termo sistema da informação é frequentemente usado para se referir à interação entre pessoas, processos, dados e tecnologia. Nesse sentido, o termo é usado para se referir não somente à tecnologia da informação e de comunicações (TIC) que uma organização usa, mas também à forma como as pessoas interagem com essa tecnologia em apoio aos processos de negócio;

• Terceiro – a pessoa que é reconhecida como sendo independente das outras partes envolvidas, até onde diz respeito o assunto em questão;

• Tratamento de riscos – é o processo de seleção e implementação de medidas para modificar os riscos. O tratamento de riscos pode envolver:

  - o Evitar o risco ao optar por não começar ou continuar com a atividade que dá origem ao risco;
  - o Tomar ou elevar o risco a fim de perseguir uma oportunidade;
  - o Remover a fonte de risco;
  - o Alterar a probabilidade;
  - o Alterar as consequências;
  - o Dividir o risco com um terceiro ou terceiros (incluindo contratos e financiamento do risco);
  - o Manter o risco através de uma escolha consciente;

• Vulnerabilidade – fraqueza de um ativo ou controle que pode ser explorada por uma ou mais ameaças.

Referências Bibliográficas:

Capeletti, Lucas. Fundamentos de Gestão de Acesso e Identidade (IAM) (Portuguese Edition).
Lisboa Melo, Jefferson; Vieira de Oliveira, Alexandre; Mauser, Daniel. Do Iniciante ao Profissional em Segurança Cibernética. SF Editorial e AcademiaTI.
Fernandes, Victor. Inteligência Artificial para Leigos (Portuguese Edition).
Wendt, Emerson; Jorge, Higor Vinicius Nogueira. Crimes Cibernéticos 3a edição: Ameaças e procedimentos de investigação (Portuguese Edition). BRASPORT.
Baars, Hans; Hintzbergen, Kees; Hintzbergen, Jule; Smulders, André. Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002 (Portuguese Edition). BRASPORT.
R., Raphael. Segurança Cibernética: Protegendo Infraestruturas e Dados (Portuguese Edition).

CYBER
ACADEMY

FEBRABAN