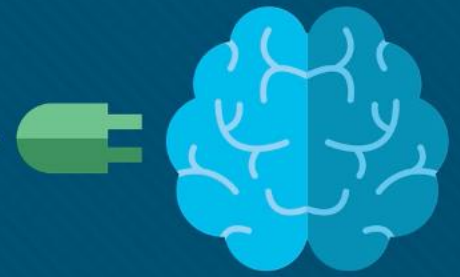


Módulo 1: Introdução à Cibersegurança

Objetivos do Módulo

Título do Módulo: Introdução à Cibersegurança

Objetivo do Módulo: Explicar o básico de manter a segurança online, incluindo o que é cibersegurança e seu impacto potencial.

Título do Tópico	Objetivo do Tópico
O mundo da segurança cibernética	Explicar o que é segurança cibernética e o possível impacto.
Dados organizacionais	Identificar os tipos de informações confidenciais que os hackers podem usar para invadir a privacidade e/ou prejudicar a reputação, onde podem acessar essas informações e por que elas são interessantes para os criminosos cibernéticos.
O que foi roubado?	Explicar o que são dados corporativos e por que devem ser protegidos.
Invasores cibernéticos	Descrever quem são os invasores cibernéticos e o que eles querem.
Guerra cibernética	Explicar o que é guerra cibernética e o motivo pelo qual as nações e os governos precisam de profissionais de segurança cibernética para ajudá-los a proteger os cidadãos e a infraestrutura.

1.1 O Mundo da Cibersegurança

O que é a Cibersegurança?

- A cibersegurança é o esforço contínuo para proteger indivíduos, organizações e governos contra ataques digitais, protegendo sistemas em rede e dados contra uso não autorizado ou danos.

- **Pessoal:** Em um nível pessoal, você precisa proteger sua identidade, seus dados e seus dispositivos de computação.

- **Organizacional:** Em nível organizacional, é responsabilidade de todos proteger a reputação da organização, seus dados e clientes.

- **Governo**: À medida que mais informações digitais são coletadas e compartilhadas, sua proteção se torna ainda mais vital no nível governamental, onde a segurança nacional, a estabilidade econômica e a segurança e bem-estar dos cidadãos estão em jogo.

Protegendo seu Dados Pessoais

- Os dados pessoais são quaisquer informações que possam ser usadas para identificá-lo e que possam existir tanto offline quanto online.

- **Identidade off-line**
  - É a persona da vida real que você apresenta diariamente em casa, na escola ou no trabalho.
  - Como resultado, a família e os amigos sabem detalhes sobre sua vida pessoal, incluindo seu nome completo, idade e endereço.
  - É importante não esquecer a importância de proteger sua identidade offline.
  - Quando você não está olhando, os ladrões de identidade podem roubar seus dados com facilidade!

- **Identidade on-line**
  - Não é apenas um nome, é quem você é e como se apresenta aos outros online.
  - Inclui o nome de usuário ou apelido que você usa para suas contas online, bem como a identidade social que você estabelece e retrata em comunidades e sites online.
  - Você deve tomar cuidado para limitar a quantidade de informações pessoais que revela por meio da sua identidade online.

Seus Dados

- Dados pessoais descrevem qualquer informação sobre você (nome, número de seguro social, número da carteira de motorista, data e local de nascimento, nome de solteira da sua mãe, fotos ou mensagens trocadas com outros).
- Cibercriminosos podem usar essas informações sensíveis para identificar e se passar por você, infringindo sua privacidade e potencialmente causando danos sérios à sua reputação.

Os hackers podem colocar as mãos nos seus dados pessoais por meio de registros, incluindo:

Registros médicos	Toda vez que você visita o médico, informações pessoais relacionadas à sua saúde física e mental e bem-estar são adicionadas aos seus registros eletrônicos de saúde (EHRs). Como a maioria desses registros são salvos on-line, você precisa estar ciente das informações médicas que compartilha. E esses registros vão além dos limites do consultório médico.
Registros de educação	Os registros educacionais contêm informações sobre suas qualificações acadêmicas e realizações. Isso também pode incluir suas informações de contato, registros de presença, relatórios disciplinares, registros de saúde e imunização, bem como quaisquer registros de educação especial, incluindo programas de educação individualizados (IEPs).
Registros de empregos e financeiros	Dados de emprego podem ser valiosos para hackers se eles conseguirem informações sobre seus empregos anteriores - ou até mesmo suas avaliações de desempenho atuais. Seus registros financeiros podem incluir informações sobre sua renda e despesas. Seus registros fiscais podem incluir contracheques, extratos de cartão de crédito, sua pontuação de crédito e detalhes da sua conta bancária.

Onde Estão os Meus Dados?

Imagine que ontem você compartilhou algumas fotos do seu primeiro dia de trabalho com alguns de seus amigos próximos.Mas isso deve estar OK, certo? Vamos ver...

- Você tirou algumas fotos no trabalho usando seu telefone celular.
- Cópias dessas fotos estão disponíveis no seu dispositivo móvel.
- Você os compartilhou com cinco amigos próximos, que moram em vários locais do mundo.
- Todos os seus amigos baixaram as fotos e agora têm cópias delas nos dispositivos.
- Um de seus amigos ficou tão orgulhoso que decidiu publicar e compartilhar suas fotos on-line.
- As fotos não estão mais apenas no seu dispositivo.
- Elas acabaram, na verdade, em servidores localizados em diferentes partes do mundo e pessoas que você nem conhece agora têm acesso às suas fotos.

O que mais?

- Este é apenas um exemplo que nos lembra que toda vez que coletamos ou compartilhamos dados pessoais, devemos considerar nossa segurança.
- Existem diferentes leis que protegem a privacidade e os dados no seu país.
- Você sabe onde estão seus dados?
  - Após uma consulta, o médico atualizará seu prontuário médico.
    - Para fins de faturamento, essas informações podem ser compartilhadas com a seguradora.
    - Nesses casos, seu prontuário médico, ou parte dele, agora pode ser acessado pela seguradora.
  - Cartões de fidelidade de lojas podem ser uma maneira conveniente de economizar dinheiro em suas compras.
    - No entanto, a loja está usando este cartão para criar um perfil do seu comportamento de compra, que pode ser usado para direcioná-lo com ofertas especiais de seus parceiros de marketing.

Dispositivos Inteligentes

- Considere a frequência com que você usa seus dispositivos de computação para acessar seus dados pessoais.
- A menos que tenha optado por receber extratos em papel, você provavelmente acessa cópias digitais de extratos de conta bancária no site do seu banco.
- E ao pagar uma conta, é muito provável que você tenha transferido os fundos necessários por meio de um aplicativo bancário no telefone celular.
- Além de permitir acessar suas informações, os dispositivos de computação também podem gerar informações sobre você.
- Tecnologias vestíveis, como smartwatches e rastreadores de atividade, coletam seus dados para pesquisa clínica, monitoramento da saúde do paciente e rastreamento de condicionamento físico e bem-estar.
- À medida que o mercado global de rastreadores de fitness cresce, também aumenta o risco para seus dados pessoais.

Roubo de Identidade

- Não contentes em roubar seu dinheiro para obter ganhos financeiros de curto prazo, os criminosos digitais investem no ganho de longo prazo do roubo de identidade.

Furto de dados médicos

- O aumento dos custos médicos levou a um aumento no roubo de identidade médica, com criminosos digitais roubando seguros médicos para usar os benefícios para si mesmos.
- Onde isso acontecer, todos os procedimentos médicos realizados em seu nome serão salvos em seus registros médicos.

Atividade bancária

- Roubar dados privados pode ajudar cibercriminosos a acessar contas bancárias, cartões de crédito, perfis sociais e outras contas online.
- Armado com essa informação, um ladrão de identidade poderia apresentar uma declaração de imposto falsa e receber o reembolso.
- Eles podem até contrair empréstimos em seu nome e arruinar sua classificação de crédito (e sua vida também).

Quem mais Quer Meus Dados?

- Não são apenas os criminosos que buscam seus dados pessoais.
- A tabela descreve outras entidades interessadas em sua identidade on-line e o motivo.

Seu provedor de serviços de Internet.	Seu ISP rastreia sua atividade on-line e, em alguns países, pode vender esses dados para os anunciantes com fins lucrativos.Em certas circunstâncias, os ISPs podem ser legalmente obrigados a compartilhar suas informações com agências ou autoridades de vigilância do governo.
Anunciantes	A publicidade direcionada faz parte da experiência na internet. Anunciantes monitoram e rastreiam suas atividades online, como hábitos de compras e preferências pessoais, e enviam anúncios direcionados para você.
Mecanismos de pesquisa e plataformas de mídia social	Essas plataformas coletam informações sobre gênero, localização geográfica, número de telefone e ideologias políticas e religiosas com base em seus históricos de pesquisa e identidade online. Essas informações são então vendidas para anunciantes visando lucro.
Sites que você visita	Os sites usam cookies para rastrear suas atividades e proporcionar uma experiência mais personalizada. Mas isso deixa um rastro de dados que está vinculado à sua identidade online e muitas vezes pode parar nas mãos de anunciantes!

1.2 Dados Corporativos

Tipo dos Dados Corporativos

Dados tradicionais geralmente são gerados e mantidos por todas as organizações, grandes e pequenas.

- Ele inclui o seguinte:
  - **Dados transacionais**, como detalhes relacionados à compra e venda, atividades de produção e operações organizacionais básicas, incluindo informações usadas para tomar decisões de emprego.
  - **Propriedade intelectual**, como patentes, marcas registradas e planos de novos produtos, permite que uma empresa obtenha vantagem econômica sobre seus concorrentes. Essas informações são geralmente consideradas um segredo comercial e perdê-las pode ser desastroso para o futuro de uma empresa.
  - **Dados financeiros**, como demonstrações de renda, balanços patrimoniais e demonstrações de fluxo de caixa, fornecem insights sobre a saúde de uma empresa.

Tipos de Dados Organizacionais (Cont.)

A Internet das Coisas (IoT) e Big Data

- **A IoT** (Internet das Coisas) é uma grande rede de objetos físicos, como sensores, software e outros equipamentos.
- Todas essas “coisas” estão conectadas à Internet, com a capacidade de coletar e compartilhar dados.
- As opções de armazenamento de dados estão se expandindo por meio da nuvem e da virtualização.
- O surgimento da IoT levou a um crescimento exponencial dos dados, criando uma nova área de interesse em tecnologia e negócios chamada "Big Data".

O Cubo

Esse modelo de segurança tem três dimensões:

1. **Os princípios fundamentais para proteger sistemas de informação**

- **Confidencialidade** é um conjunto de regras que impede que informações confidenciais sejam divulgadas a pessoas, recursos e processos não autorizados. Os métodos para garantir a confidencialidade incluem **criptografia de dados**, **comprovação de identidade** e **autenticação de dois fatores**.

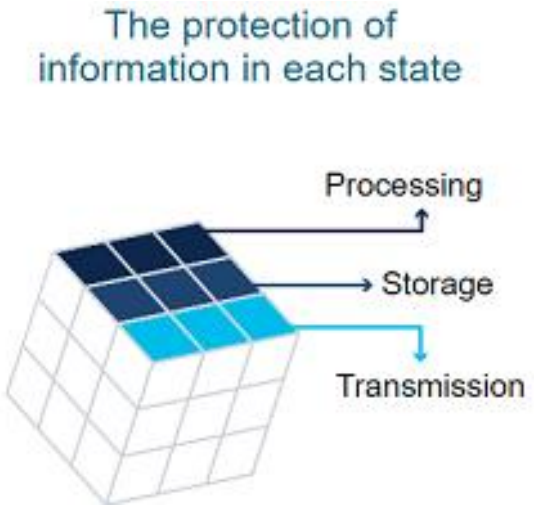
- **A integridade** garante que as informações ou processos do sistema sejam protegidos contra modificações intencionais ou acidentais. Uma maneira de garantir isso é usar uma **função de hash** ou **checksum**.

- Disponibilidade significa que os usuários autorizados podem acessar sistemas e dados quando e onde necessário, e aqueles que não atendem às condições estabelecidas, não podem. Isso pode ser alcançado por manutenção de equipamentos, realizando reparos de hardware, **mantendo os sistemas operacionais** e **software atualizadose criando de backups**.

O Cubo (cont.)

2. **A proteção das informações em cada um de seus possíveis estados.**

   - **O processamento** refere-se aos dados que estão sendo usados para executar uma operação, como atualizar um registro de banco de dados (dados em processo).
   - **Armazenamento** refere-se a dados armazenados na memória ou em um dispositivo de armazenamento permanente, como um disco rígido, unidade de estado sólido ou pen drive (dados em repouso).
   - **Transmissão** refere-se a dados que viajam entre sistemas de informação (dados em trânsito).



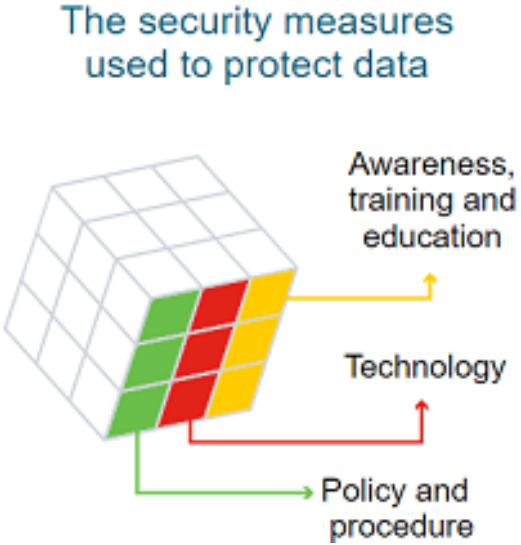
O Cubo (cont.)

3. **As medidas de segurança usadas para proteger dados**

- **Conscientização, treinamento e educação** são as medidas implementadas por uma organização para garantir que os usuários estejam cientes das potenciais ameaças à segurança e das ações que podem tomar para proteger os sistemas de informação.

- **Tecnologia** refere-se às soluções baseadas em software e hardware projetadas para proteger sistemas de informação, como firewalls, que monitoram continuamente sua rede em busca de possíveis incidentes maliciosos.

- **Políticas e procedimentos** referem-se aos controles administrativos que fornecem uma base para como uma organização implementa a segurança da informação, como planos de resposta a incidentes e diretrizes de melhores práticas.



Isso é Real?

- O phishing é muito comum e geralmente funciona.
- Por exemplo, em agosto de 2020, a marca de jogos de elite Razer sofreu uma violação de dados que expôs as informações pessoais de aproximadamente 100.000 clientes.
- Um consultor de segurança descobriu que um cluster de nuvem (um grupo de servidores vinculados fornecendo armazenamento de dados, bancos de dados, redes e software através da Internet) foi configurado incorretamente e expôs um segmento da infraestrutura da Razer à Internet pública, resultando em um vazamento de dados.
- Levou mais de três semanas para a Razer garantir que a instância na nuvem não estivesse acessível ao público, durante as quais cibercriminosos tiveram acesso a informações de clientes que poderiam ter sido usadas em ataques de engenharia social e fraudes.
- Portanto, as organizações precisam adotar uma abordagem proativa para a segurança na nuvem, garantindo que dados sensíveis estejam protegidos.

Violacões de Segurança de Dados

- As violações de segurança de dados estão se tornando cada vez mais comuns, e as implicações são severas.
- A IoT está conectando cada vez mais dispositivos, criando mais oportunidades para os criminosos digitais atacarem.
- Duas violações de segurança de dados conhecidas incluem:

  - **O botnet Persirai**
    - Em 2017, um botnet da Internet das Coisas (IoT), Persirai, teve como alvo mais de 1.000 modelos diferentes de câmeras IP, acessando portas abertas para injetar um comando que obrigou as câmeras a se conectarem a um site que instalou malware nelas.
    - Depois que o malware foi baixado e executado, ele se excluiu e, portanto, foi capaz de ser executado na memória para evitar a detecção.
    - Mais de 122.000 dessas câmeras de vários fabricantes foram sequestradas e usadas para realizar ataques DDoS, sem o conhecimento de seus proprietários.
    - Um ataque de DDoS ocorre quando vários dispositivos infectados por malware inundam os recursos de um sistema visado.

Violações de Segurança de Dados (cont.)

- **Equifax Inc.**
  - Em setembro de 2017, a Equifax, uma agência de relatórios de crédito ao consumidor nos EUA, anunciou publicamente um evento de violação de dados: os atacantes conseguiram explorar uma vulnerabilidade em seu software de aplicação web para obter acesso aos dados pessoais sensíveis de milhões de clientes.
  - Em resposta a essa violação, a Equifax criou um site dedicado que permitiu que seus clientes determinassem se suas informações estavam comprometidas.
  - O uso de um novo nome de domínio, em vez de usar um subdomínio equifax.com, permitiu que os criminosos criassem sites não autorizados com nomes semelhantes.
  - Esses sites foram usados para enganar os clientes e fornecer informações pessoais.
  - Os invasores podem usar essas informações para assumir a identidade de um cliente.
  - Nesses casos, seria muito difícil para o cliente provar o contrário, já que o hacker também está ciente de suas informações pessoais.

Consequências de uma Violação de Segurança

Esses exemplos mostram que as possíveis consequências de uma violação de segurança podem ser

Danos à reputação	Uma violação de segurança pode ter um impacto negativo a longo prazo na reputação de uma empresa que levou anos para ser construída. Os clientes, especialmente aqueles que foram afetados negativamente pela violação, precisarão ser notificados e poderão buscar uma compensação e / ou recorrer a um concorrente confiável e seguro. Os funcionários também podem optar por sair devido a um escândalo. Dependendo da gravidade de uma violação, pode levar muito tempo para reparar a reputação de uma empresa.
Vandalismo	Um hacker ou um grupo de hackers pode vandalizar o site de uma empresa publicando informações falsas. Eles podem até fazer algumas edições menores no número de telefone ou no endereço da empresa, o que pode ser mais difícil de detectar. Em ambos os casos, o vandalismo on-line pode retratar o não profissionalismo e ter um impacto negativo na reputação e na credibilidade da sua organização.
Roubo	Uma violação de dados geralmente envolve um incidente em que dados pessoais confidenciais foram roubados. Os criminosos digitais podem tornar essas informações públicas ou explorá-las para roubar dinheiro e/ou identidade de um indivíduo.
Perda de receita	O impacto financeiro de uma violação de segurança pode ser devastador. Por exemplo, os hackers podem derrubar o site de uma empresa, impedindo-o de fazer negócios online. A perda de todas essas informações pode impedir a expansão e o crescimento da empresa. Pode exigir mais investimento na infraestrutura de segurança de uma empresa. E não vamos esquecer que as empresas podem enfrentar grandes multas ou penalidades se não protegerem os dados online.
Propriedade intelectual prejudicada	Uma violação de segurança também pode ter um impacto devastador na competitividade de uma empresa, principalmente se os hackers conseguirem obter documentos confidenciais, segredos comerciais e propriedade intelectual.

1.3 O Que Foi Levado?

Cenário 1

- Hoje, as violações de segurança são muito comuns, com os invasores constantemente encontrando maneiras novas e inovadoras de se infiltrar nas empresas em busca de informações valiosas.
- Considere os seguintes dois cenários fictícios.

Cenário 1:

- De acordo com nossas fontes, uma conhecida cadeia de hotéis que opera em todo o mundo relatou uma violação de dados enorme, com as informações pessoais de mais de três milhões de hóspedes expostas a hackers.

- O hotel descobriu que os hackers obtiveram acesso ao banco de dados de clientes usando os detalhes de login de um de seus funcionários.

- Neste momento, o hotel não acredita que os hackers puderam acessar senhas de contas ou informações financeiras.

- Hóspedes recentes são incentivados a verificar o portal web da cadeia de hotéis para ver se eles foram afetados por essa violação.

Cenário 2

Cenário 2:

- A equipe da @Apollo está preocupada. As plataformas de eLearning estão se tornando os principais alvos dos invasores, à medida que mais e mais empresas migram para a aprendizagem digital.
- Uma plataforma de treinamento on-line popular admitiu ter deixado os dados pessoais de milhões de seus alunos (muitos deles menores) expostos em um banco de dados em nuvem publicamente acessível.
- Os hackers conseguiram acessar diretamente os nomes completos dos alunos, endereços de e-mail, números de telefone e detalhes de matrícula na escola pela Internet!
- Embora não esteja claro o que os hackers fizeram com essas informações adquiridas, é seguro dizer que eles têm tudo o que precisam para realizar ataques generalizados de phishing ou malware.

Pontos Principais

- Uma violação de segurança é um incidente que resulta em acesso não autorizado a dados, aplicações, serviços ou dispositivos, expondo informações privadas que os invasores podem usar para ganho financeiro ou outras vantagens.
- Mas há muitas maneiras de proteger você e sua empresa.
- É importante estar ciente das ameaças digitais comuns e permanecer vigilante para que você não se torne a próxima vítima.

Descubra Mais

Pesquise alguns exemplos adicionais de violações de segurança recentes.

- Em cada caso, você pode identificar:
  - o que foi tirado?
  - quais explorações os invasores usaram?
  - quais ações podem ser tomadas para evitar que a violação ocorra novamente no futuro?

1.4 Invasores Cibernéticos

Tipos de Invasores

- Os invasores cibernéticos variam de amadores a organizados e farão de tudo para colocar as mãos em informações pessoais.
- Eles são frequentemente classificados como invasores white hat, gray hat ou black hat.

Hackers amadores

- O termo 'script kiddies' surgiu na década de 90 e refere-se a hackers amadores ou inexperientes que usam ferramentas existentes ou instruções encontradas na Internet para lançar ataques.
- Alguns script kiddies são apenas curiosos, outros estão tentando demonstrar suas habilidades e causar danos.
- Embora esses invasores possam usar ferramentas básicas, os ataques ainda podem ter consequências devastadoras.

Tipos de Atacantes (Cont.)

Hackers

- Esse grupo de atacantes invade sistemas de computadores ou redes para obter acesso.
- Dependendo da intenção da invasão, elas podem ser classificadas da seguinte forma:
  - **Atacantes white hat** invadem redes ou sistemas de computadores para identificar quaisquer vulnerabilidades, de modo que a segurança de um sistema ou rede possa ser aprimorada. Essas invasões são realizadas com permissão prévia e quaisquer resultados são relatados ao proprietário.
  - **Atacantes gray hat** podem procurar vulnerabilidades em um sistema, mas só relatarão suas descobertas aos proprietários do sistema se isso estiver alinhado com sua agenda. Alguns hackers gray hat publicam os fatos sobre a vulnerabilidade na Internet para que outros invasores possam explorá-la.
  - **Invasores black hat** tiram vantagem de qualquer vulnerabilidade para obter ganhos pessoais, financeiros ou políticos ilegais.

Tipos de Atacantes (Cont.)

Hackers organizados

- Esses criminosos incluem organizações de hacktivistas, criminosos virtuais, terroristas e os hackers patrocinados pelo Estado.
- Os criminosos são altamente sofisticados e organizados e ainda podem fornecer o crime digital como um serviço a outros criminosos.
- Os hacktivistas fazem declarações políticas para sensibilizar para questões que são importantes para eles.
- Os invasores patrocinados pelo estado reúnem informações ou cometem sabotagem em nome de seu governo.
- Eles geralmente são altamente treinados e bem financiados, e seus ataques são focados em objetivos específicos que são benéficos para seu governo.

Ameaças Internas e Externas

- Os ataques cibernéticos podem se originar dentro e fora da empresa.

- **Interno**
  - Funcionários, contratados ou parceiros confiáveis podem, acidental ou intencionalmente:
    - manipular dados confidenciais de forma incorreta
    - facilitar ataques externos conectando mídia USB infectada ao sistema de computador da organização
    - introduzir malware na rede da organização ao clicar em e-mails ou sites maliciosos
    - ameaçar as operações de servidores internos ou dispositivos de infraestrutura de rede

- **Externo**
  - Os amadores ou invasores qualificados fora da empresa podem:
    - explorar vulnerabilidades na rede
    - obter acesso não autorizado a dispositivos de computação
    - usar a engenharia social para obter acesso não autorizado a dados organizacionais.

1.5 Guerra Cibernética

Sinal dos Tempos (Stuxnet)

- Um exemplo de ataque patrocinado pelo estado envolveu o malware Stuxnet, que foi projetado não apenas para invadir computadores de destino , mas também para causar danos físicos a equipamentos controlados por computadores!

- Assista a um vídeo curto sobre o caso do Stuxnet e descubra o impacto que esse malware teve na planta de enriquecimento nuclear do Irã.

O Propósito da Guerra Cibernética

- A principal razão para recorrer à ciberguerra é obter vantagem sobre adversários, sejam eles nações ou concorrentes.
- A guerra cibernética é usada das seguintes maneiras:

- **Para coletar informações comprometidas e/ou segredos de defesa**

  - Uma nação ou organização internacional pode se envolver em uma guerra cibernética para roubar segredos de defesa e obter informações sobre tecnologias que ajudarão a reduzir as lacunas em suas indústrias e capacidades militares.

  - Além disso, dados sensíveis comprometidos podem dar aos atacantes uma alavanca para chantagear pessoal dentro de um governo estrangeiro.

O Propósito da Guerra Cibernética (Cont.)

- **Para impactar a infraestrutura de outra nação**
  - Além da espionagem industrial e militar, uma nação pode invadir continuamente a infraestrutura de outra nação para causar disrupção e caos.
  - Por exemplo, um ataque pode interromper a rede de energia de uma grande cidade.
  - Considere as consequências se isso acontecesse; as estradas estariam congestionadas, a troca de bens e serviços seria interrompida, os pacientes não conseguiriam receber o cuidado necessário em caso de emergência, o acesso à internet seria interrompido.
  - Ao desligar uma rede elétrica, um ataque digital pode ter um grande impacto no dia a dia dos cidadãos comuns.

1.6 Questionário de Módulo

O Que Aprendi Neste Módulo?

- A cibersegurança é o esforço contínuo para proteger indivíduos, organizações e governos contra ataques digitais, protegendo sistemas em rede e dados contra uso não autorizado ou danos.
- Os dados pessoais são quaisquer informações que possam ser usadas para identificá-lo e que possam existir tanto offline quanto online.
- Os dados tradicionais são normalmente gerados e mantidos por todas as organizações, grandes e pequenas.
- O Cubo McCumber é um modelo estrutural criado por John McCumber em 1991 para ajudar as organizações a estabelecer e avaliar iniciativas de segurança da informação, considerando todos os fatores relacionados que as impactam.
- Uma violação de segurança pode ter um impacto negativo de longo prazo na reputação de uma organização que levou anos para ser construída.
- Uma violação de dados frequentemente envolve um incidente em que dados pessoais sensíveis foram roubados.
- Cibercriminosos podem tornar essa informação pública ou explorá-la para roubar o dinheiro e/ou a identidade de um indivíduo.
- Os ataques cibernéticos podem se originar tanto de dentro de uma organização quanto de fora dela.