SEGURANÇA CIBERNÉTICA

PROF. ENG. DANIEL JOSÉ PIMENTA

PRINCÍPIOS E CONCEITOS DE SEGURANÇA CIBERNÉTICA

A EVOLUÇÃO DA SEGURANÇA CIBERNÉTICA

PRINCÍPIOS E CONCEITOS DE SEGURANÇA CIBERNÉTICA

A EVOLUÇÃO DA SEGURANÇA CIBERNÉTICA

1995 a 2007

- Internet, Sistemas Operacionais +facilidade, a disponibilidade supera a necessidade...resta equacionar o uso...

2007 até hoje

- Convergência Digital, Equipamentos Wireless de multiuso, câmera, vídeo, som…tudo em um equipamento - personalização(Tablet e Smartphone)

QUANTOS ANOS CADA MÍDIA LEVOU PARA CONQUISTAR 50 MILHÕES DE USUÁRIOS

70 anos

38 anos

13 anos

05 anos

OBRIGA

O que muda é o tempo!

PRINCÍPIOS E CONCEITOS DE SEGURANÇA CIBERNÉTICA

A EVOLUÇÃO DA SEGURANÇA CIBERNÉTICA

O Creeper e o Reaper, 1971

O Creeper, considerado o primeiro vírus do mundo, era um código portátil que podia viajar entre sistemas Tenex. Ele tinha como alvo os computadores mainframe PDP-10 da Corporação de Equipamentos Digitais (DEC) conectados ao Arpanet e imprimiu "Eu sou o creeper: pegue-me se puder" no teletipo modelo 33 ASR. Ele não afetou nenhum efeito destrutivo de longo prazo nos dispositivos afetados.

Reaper é uma versão aprimorada de auto-replicação do Creeper, que foi projetada para se mover pela Arpanet, excluindo cópias do Creeper. É considerado o primeiro programa antivírus do mundo.

https://blogs.manageengine.com/portugues/2021/02/27/evolucao-da-ciberseguranca-uma-breve-linha-do-tempo.html
https://www.youtube.com/watch?v=o751LKmZCg8

PRINCÍPIOS E CONCEITOS DE SEGURANÇA CIBERNÉTICA
A EVOLUÇÃO DA SEGURANÇA CIBERNÉTICA

O primeiro congelamento de rede, 1988

Um erro inadvertido em um código de worm projetado para medir o tamanho da Internet resultou no primeiro ataque DoS. O erro fez com que o Worm Morris se replicasse incessantemente a ponto de a Internet inicial (Arpanet) ficar entupida e 10% de todos os sistemas conectados travar. Robert T. Morris, o criador do Worm Morris, tornou-se a primeira pessoa a ser acusada de acordo com a Lei de Fraude e Abuso de Computador.

PRINCÍPIOS E CONCEITOS DE SEGURANÇA CIBERNÉTICA

A EVOLUÇÃO DA SEGURANÇA CIBERNÉTICA

Diz a lenda que o estudante da Universidade de Cornell, Robert Tappan Morris, decidiu "medir o tamanho da Internet". Para realizar essa pesquisa, ele escreveu um programa bastante complicado que foi capaz de reproduzir a si mesmo através da rede sem ser detido. É fácil notar que esta funcionalidade corresponde exatamente com a definição de vírus de computador. O Morris worm não foi desenvolvido para causar danos, no entanto um erro de programação levou a infecções múltiplas a partir de um único computador, deixando o servidor sobrecarregado e sem resposta.

PRINCÍPIOS E CONCEITOS DE SEGURANÇA CIBERNÉTICA

A EVOLUÇÃO DA SEGURANÇA CIBERNÉTICA

Apesar de não estarem preparados técnicamente e conceitualmente, os administradores de sistemas americanos agiram rapidamente. Dois grupos de trabalho foram criados e levaram apenas dois dias para encontrar e corrigir as vulnerabilidades utilizadas pelo malware para destruí-lo com a mesma receita. Ou seja, era o fim do sem-fim. Porém, o custo da remoção dessa infecção foi de aproximadamente US$ 10 milhões.

PRINCÍPIOS E CONCEITOS DE SEGURANÇA CIBERNÉTICA

A EVOLUÇÃO DA SEGURANÇA CIBERNÉTICA

O esforço de Morris para permanecer anônimo poderia ter sido bem sucedido. A pessoa que não permitiu isso foi seu pai, Robert Morris, co-autor e cientista-chefe do National Computer Security Center da NSA, que convenceu seu filho a confessar. O tribunal levou isso em conta, e a sentença de Morris júnior foi suave: três anos de liberdade condicional, US$ 10 mil e 400 horas de serviço comunitário. Esta lição foi útil para Morris. Ao final da história, ele se tornou um membro respeitado na setor da computação. Entre suas realizações estão: a criação de um dos primeiros e-commerce, o desenvolvimento de novas linguagens de programação, e o cargo de professor no MIT.

PRINCÍPIOS E CONCEITOS DE SEGURANÇA CIBERNÉTICA
A EVOLUÇÃO DA SEGURANÇA CIBERNÉTICA

O Departamento de Segurança Interna, 2002

O Departamento de Segurança Interna dos Estados Unidos, estabelecido pelo presidente George W. Bush em 2002, assumiu a responsabilidade de proteger a infraestrutura de TI crucial dos Estados Unidos. Em 2018, Donald Trump sancionou a Lei da Agência de Segurança de Infraestrutura e Segurança Cibernética que deu origem ao Agência de Segurança Cibernética e Infraestrutura (CISA). A CISA trabalha com o governo federal na defesa contra ataques cibernéticos.

PRINCÍPIOS E CONCEITOS DE SEGURANÇA CIBERNÉTICA

A EVOLUÇÃO DA SEGURANÇA CIBERNÉTICA

O nascimento do Anonymous, 2003

Anonymous foi, de longe, o grupo hacktivista mais popular, que estreou no quadro de imagens do 4chan. Ele é um coletivo internacional descentralizado que realiza ataques cibernéticos como um meio de chamar a atenção para suas visões políticas e expor alvos de alto perfil.

PRINCÍPIOS E CONCEITOS DE SEGURANÇA CIBERNÉTICA

A EVOLUÇÃO DA SEGURANÇA CIBERNÉTICA

Operação Aurora, 2009

A Operação Aurora foi uma série de ataques cibernéticos originados na China e direcionados às informações de propriedade intelectual de mais de trinta empresas do setor privado dos EUA, incluindo Google, Yahoo e Adobe. Este incidente trouxe à luz as capacidades das operações cibernéticas como uma ferramenta para realizar espionagem industrial em grande escala.

PRINCÍPIOS E CONCEITOS DE SEGURANÇA CIBERNÉTICA

A EVOLUÇÃO DA SEGURANÇA CIBERNÉTICA

Stuxnet, 2010

O Stuxnet era um worm de computador extremamente sofisticado que explorava várias vulnerabilidades zero-day do Windows. Supostamente criado por um programa secreto dos EUA-Israel, ele teve como alvo e destruiu centrífugas na instalação de enriquecimento de urânio em Natanz, Irã, causando danos substanciais ao programa nuclear do país.

PRINCÍPIOS E CONCEITOS DE SEGURANÇA CIBERNÉTICA
A EVOLUÇÃO DA SEGURANÇA CIBERNÉTICA

EternalBlue e ataques ransomware, 2017

EternalBlue é um exploit que utiliza vulnerabilidades na implementação do Windows do protocolo Server Message Block (SMB). Foi divulgado pelo grupo de hackers Shadow Brokers em abril de 2017. Dois grandes surtos de ransomware em todo o mundo, WannaCry e NotPetya, usaram esse exploit para afetar computadores sem patch.

PRINCÍPIOS E CONCEITOS DE SEGURANÇA CIBERNÉTICA
A EVOLUÇÃO DA SEGURANÇA CIBERNÉTICA

Regulamento Geral de Proteção de Dados (GDPR), 2018

O Regulamento Geral de Proteção de Dados (GDPR) é um regulamento de conformidade que fornece aos cidadãos da União Europeia (UE) maior controle sobre seus dados pessoais. Ao abrigo deste mandato, as organizações são responsáveis pela proteção dos dados pessoais e da privacidade dos cidadãos da UE. O GDPR se aplica não apenas a todas as organizações que operam na UE, mas também a organizações que oferecem bens ou serviços a clientes ou empresas na UE. Foi aprovado pelo Parlamento Europeu em abril de 2016 e entrou em vigor em 25 de maio de 2018.

PRINCÍPIOS E CONCEITOS DE SEGURANÇA CIBERNÉTICA

A EVOLUÇÃO DA SEGURANÇA CIBERNÉTICA

O hack do Twitter, 2020

Um dos incidentes de segurança cibernética mais sensacionais deste ano aconteceu quando as contas de vários usuários de alto perfil do Twitter foram hackeadas, incluindo as de Barack Obama, Elon Musk e Bill Gates. Os hackers postaram tweets fraudulentos que diziam “Estou retribuindo à comunidade. Todos os Bitcoins enviados para o endereço abaixo serão devolvidos em dobro! Se você enviar $ 1.000, eu irei devolver $ 2.000. Só fazendo isso por 30 minutos” e ganharam £ 86.800 em poucas horas. A violação se enquadra na categoria de ameaça interna e, quer envolva as ações de um insider malicioso ou funcionário negligente, prova que os humanos são o elo mais fraco na cadeia de segurança cibernética.

PRINCÍPIOS E CONCEITOS DE SEGURANÇA CIBERNÉTICA

A EVOLUÇÃO DA SEGURANÇA CIBERNÉTICA

Trabalho remoto – A nova norma, mais recursos de segurança chegando em 2021

Na esteira da pandemia COVID-19, a maioria das empresas foi forçada a adotar um modelo de trabalho remoto. Embora a transição para muitas organizações tenha sido difícil, as indicações são de que os cenários de trabalho remoto provavelmente permanecerão em vigor mesmo após o fim da pandemia. Embora já tenha havido um aumento nas ferramentas de trabalho remoto que permitem uma colaboração tranquila entre as equipes, o aspecto da segurança está evoluindo rapidamente agora e continuará nos anos seguintes. Procedimentos de autenticação multifator integrados, melhores técnicas de criptografia e o uso de redes virtuais privadas se tornarão comuns.

PRINCÍPIOS E CONCEITOS DE SEGURANÇA CIBERNÉTICA
A EVOLUÇÃO DA SEGURANÇA CIBERNÉTICA

Segurança cibernética habilitada para inteligência artificial (IA)

Com algoritmos de aprendizado de máquina eficientes e integração perfeita de IA em aplicações de segurança cibernética, a detecção de ameaças em tempo real e a resposta automatizada a incidentes são possíveis e estão sendo continuamente aprimoradas. Mecanismos de correlação de ameaças eficazes que detectam ataques em seus estágios iniciais se tornarão mais refinados como a defesa da linha de frente para as organizações.

PRINCÍPIOS E CONCEITOS DE SEGURANÇA CIBERNÉTICA

VALOR DA INFORMAÇÃO - ALINHAMENTO ESTRATÉGICO DA SEGURANÇA AOS NEGÓCIOS

A segurança da informação deve existir para proteger os recursos de informação que são utilizados estratégica e operacionalmente para o funcionamento da organização, contra divulgação indevida, seja ela intencional ou não, alteração não autorizada, destruição não desejada, negação de serviço, fraudes financeiras, apropriação indevida de informações ou reputação da imagem da instituição. Essa proteção é feita através da implantação de controles de segurança definidos em políticas e procedimentos (LIMA, 2013, p. 14)

CONHECER OS POSSÍVEIS OPONENTES	identificando o que eles desejam fazer, e os perigos que podem vir a causar à organização;
CONTABILIZAR OS VALORES	uma vez que a implementação e o gerenciamento da política de segurança pode significar, além da necessidade de mais recursos pessoais, a necessidade de significativos recursos de software e de hardware. Os custos das medidas de segurança devem, portanto, ser compatíveis e proporcionais às necessidades da organização e às probabilidades de ocorrerem incidentes de segurança;

CONSIDERAR OS FATORES HUMANOS	uma vez que muitos procedimentos de segurança falham, porque as reações dos usuários a esses procedimentos não são considerados com seu devido valor;
CONHECER OS PONTOS FRACOS	pois todo sistema possui vulnerabilidades;
APLICAR A SEGURANÇA DE ACORDO COM OS NEGÓCIOS DA ORGANIZAÇÃO	a fim de definir uma estratégia de segurança que melhor se adapte às necessidades deles.