Curso Técnico em Desenvolvimento de Sistemas Online

SEGURANÇA DE SISTEMAS DE INFORMAÇÃO

GEEaD - Grupo de Estudo de Educação a Distância

Centro de Educação Tecnológica Paula Souza

Expediente

GEEaD – CETEC
GOVERNO DO ESTADO DE SÃO PAULO
EIXO TECNOLÓGICO DE INFORMAÇÃO E COMUNICAÇÃO
CURSO TÉCNICO EM DESENVOLVIMENTO DE SISTEMAS
TECNOLOGIA DA INFORMAÇÃO III

Autores:
Marcelo Fernando Iguchi
Eliana Cristina Nogueira Barion

Revisão Técnica:
Lilian Aparecida Bertini

Revisão Gramatical:
Juçara Maria Montenegro Simonsen Santos

Editoração e Diagramação:
Flávio Biazim

São Paulo – SP, 2019

APRESENTAÇÃO

Este material didático do Curso Técnico em Desenvolvimento de Sistemas modalidade EaD foi elaborado especialmente por professores do Centro Paula Souza para as Escolas Técnicas Estaduais – ETECs.

O material foi elaborado para servir de apoio aos estudos dos discentes para que estes atinjam as competências e as habilidades profissionais necessárias para a sua plena formação como Técnicos em Desenvolvimento de Sistemas.

Esperamos que este livro possa contribuir para uma melhor formação e apefeiçoamento dos futuros Técnicos.

AGENDA 6

SEGURANÇA EM REDES DE COMPUTADORES E DISPOSITIVOS MÓVEIS

podemos dizer que ele depende de uma falha do usuário, e por isso é um pouco mais difícil de se espalhar. Esse vírus do ciberataque foi desenvolvido em cima de uma falha de segurança do sistema Windows, por isso se espalhou globalmente, quem não tinha atualizado o Windows a partir de março foi infectado. Além disso, ele tem o organismo de replicação, o que colabora muito para a disseminação", alerta Rafael.

Backup

"É muito importante ter backup de todos os arquivos. A empresa que tinha esse backup não precisou se preocupar, pois não perdeu informações. Dependendo do segmento é importante ter um backup até em um lugar geograficamente diferente, caso haja danos em todas as máquinas da empresa", enfatiza Ricardo.

Orientação aos usuários

"O usuário é uma porta de entrada para vírus. Ele pensa que a TI pode consertar tudo, ou que o antivírus pode impedir o acesso, mas às vezes não é assim. Como foi o caso deste ciberataque, o vírus era novo, então não havia vacina", explica o diretor técnico.

Rafael completa: "É preciso orientar o usuário, dar um treinamento. O gestor deve orientá-lo a não abrir e-mails suspeitos, de pessoas que não conhecem. Na dúvida, não clique. Se não for um e-mail falso, a pessoa entrará em contato novamente".

Plano de contingência

"Esse vai ser o crime do século XXI em diante, isso será uma constante. Tem que ter em mente um programa para quando isso acontecer, para ter segurança. As empresas sofrem ataques todos os dias, é que o usuário final não sabe. É preciso estar preparado, cedo ou tarde você pode ser atacado", recomenda Ricardo.

Como se pode perceber, assim como a evolução tecnológica tem chegado a galope, a evolução dos crimes também. Não deixe de atualizar suas medidas de segurança também! Por isso, vamos mergulhar no tema dessa agenda.

Adaptado de https://ebusiness.liveuniversity.com/2017/05/16/ciberataque-minha-empresa-foi-infectada-e-agora. Acessado em 30/10/2018.

MERGULHANDO NO TEMA...

Frequentemente, quando temos problemas com os nossos computadores como: lentidão, comportamentos erráticos ou estranhos como programas abrindo e fechando sozinhos, recebimentos ou envio de mensagens de e-mail não solicitadas, colocamos a culpa nos vírus de computador.

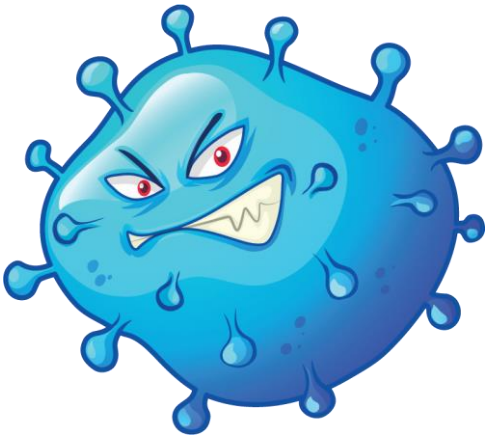
Assim que desconfiamos que o nosso computador está infectado tentamos resolver o problema o mais breve possível porque esses "vírus" podem deixar o computador mais lento para a utilização ou ainda causar grandes prejuízos financeiros e de reputação.

Todavia, existe todo um "ecossistema de pragas virtuais" além dos vírus. Só para citar temos os vírus: óbvio, os worms, bots, spyware, cavalos de tróia, ransomware, além de outros tipos de ataque. Esses vírus são classificados de acordo com o seu tipo e mecanismo de ação e propagação.

Você saberia dizer qual a diferença entre um vírus, um verme (worm) e um bot?

Perguntinha difícil, hein?! Mas vamos às explicações...

Um **Vírus** é pode ser parte de um programa de computador ou um programa completo, usualmente malicioso que realiza cópias de si mesmo infectando outros arquivos ou programas do computador. Um vírus não se propaga sozinho, ele depende da ação do usuário executar o arquivo infectado para agir contaminando o computador. Antigamente, eles se propagavam por intermédio de disquetes contaminados. Atualmente, o principal meio de disseminação dessas pragas virtuais são os pen drives e cartões de memória. Os tipos mais comuns de vírus são os vírus de macro, de script, recebidos por anexos e e-mail.



Um **Worm** ou verme é um malware capaz de se propagar sozinho, de forma automática, pela rede de comunicação enviando cópias de si mesmo automaticamente de computador para computador. Portanto, não depende da ação do usuário. Ele explora vulnerabilidades dos sistemas para se propagar. Causa muitos transtornos uma vez que consome recursos como:
tempo de processamento da CPU, memória do computador e largura de banda de redes de comunicação, dependendo da quantidade de cópias ativas simultâneas na rede.

Imagem 03

Após a infeção do computador, o worm identifica os computadores alvos para a sua replicação, depois realiza a tentativa de o envio das suas cópias para os alvos e para a ativação das cópias enviadas. Podem acontecer algumas ocorrências: como a utilização de brechas de segurança no sistema para a ativação automática, a execução de um arquivo infectado pelo usuário ou algum evento específico, como a utilização de mídias removíveis, como pen drive.

Um **Bot**, abreviação proveniente de roBOT (robô) é um programa de computador que pode ser controlado a distância e seu mecanismo de infeção é semelhante ao do worm. Quando um computador é infectado por um bot ele é, geralmente, chamado de zumbi, pois pode ser controlado remotamente, sem que o seu utilizador tenha conhecimento disso.

A pessoa que controla os bots pode formar uma rede com milhares ou milhões desses em conjunto, aí temos uma botnet. **Botnets** são frequentemente utilizadas para a realização de ataques em larga escala contra um alvo (computador, servidor ou instituição privada ou governamental) para retirá-lo de serviço.

Você viu como existem grandes diferenças entre as ameaças virtuais? Mas não existem somente essas três

citadas, vamos continuar conhecendo mais algumas:

Existem programas desenvolvidos especificamente para monitorar as atividades que o usuário desenvolve no computador. São os chamados **Spywares** ou programas espiões. Esses programas trabalham coletando dados e informações e posteriormente enviando-as para terceiros. Podem funcionar capturando o que digitamos no teclado, os chamados keyloggers, capturando telas do nosso computador, chamados de **screenloggers** ou apresentando anúncios de propagandas, os **Adwares**.

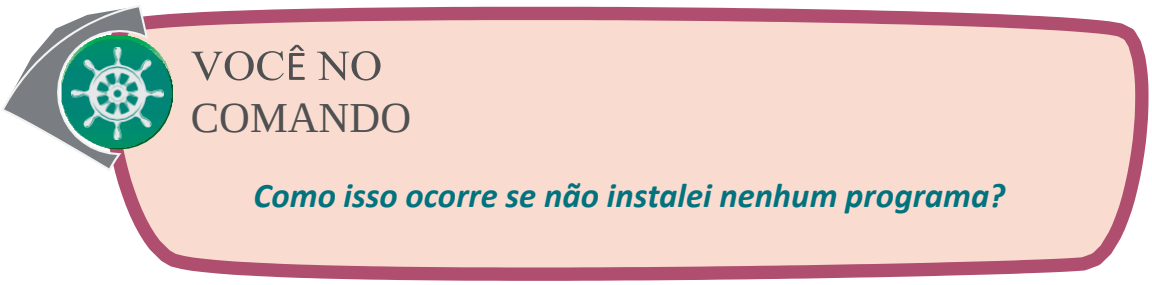
Os keyloggers e screenloggers são muito perigosos porque podem capturar os nomes de usuários e a senhas que digitamos ao acessarmos contas de e-mail e internet banking, por exemplo. Os Keyloggers armazenam as teclas digitadas pelo usuário, buscando senhas e informações importantes, já os Screenloggers armazenam os dados que se deseja coletar em forma de imagem, capturando a área que circunda a posição do mouse quando ele é clicado.

Já os adwares exibem propagandas e anúncios para o desenvolvedor do programa obter um retorno financeiro de um software que é distribuído de uma forma gratuita na internet, por exemplo. Mas então por que ele pode ser classificado como uma ameaça?

Os adwares podem ser classificados como uma ameaça porque se utilizam de mecanismos pouco confiáveis para realizar suas tarefas como: se esconder no sistema instalado para dificultar a sua remoção, enviar dados de navegação na internet e utilizar o computador sem o consentimento do usuário para direcionar os anúncios exibidos no programa e tentar melhorar a eficiência dos produtos que estão sendo ofertados.

Você não acredita em coleta de dados?

Faça uma experiência simples: vá em um site de compras de sua preferência e pesquise sobre um determinado produto, pode ser um celular, por exemplo. Veja as características de alguns modelos e depois note que quando estiver navegando na internet em outros sites que não tem nada a ver com a pesquisa, alguns estarão exibindo anúncios dos produtos que você procurou!



Bom, sempre que navegamos na internet por meio dos browsers, algumas as páginas visitadas podem armazenar arquivos individuais no nosso computador, chamados de cookies. Esses arquivos armazenam informações sobre onde clicamos no site, o que visitamos nele etc. Acontece que os cookies podem armazenam também o histórico de pesquisa que realizamos e com isso sem o nosso consentimento, alguns sites realizam a leitura desses cookies e utilizam as informações para direcionamento de propagandas e outros fins.

Quer saber mais sobre os cookies?
Acesse "Cookies - Informações que os sites armazenam no seu computador".
Link: https://support.mozilla.org/pt-BR/kb/cookies-informacoes-sites-armazenam-no-computador - acessado em 22/10/2018.

Não podemos esquecer também que existe o Cavalo de Troia, Trojan Horse ou simplesmente Trojan. Mas você sabe por que recebe esse nome?

Vamos conhecer um pouco de história: O cavalo de Troia foi um imenso cavalo de madeira construído pelos gregos e dado de presente à cidade de Troia. Esse "presente" levou a queda desta cidade, pois no interior do cavalo estava repleto de soldados gregos. Ou seja, o que aparentava ser um agrado, não era, era um ataque. Daí surgiu a expressão "presente de grego".

Em informática o princípio é o mesmo. Geralmente são programas gratuitos mal intencionados que executam as funções para as quais foi desenvolvido e anunciado como um disfarce. Além disso, realizam funções fraudulentas, agindo como os vírus, worms, bots e outros. Muitos trojans são distribuídos por e-mails falsos.

Antispam.br – 2/4 – Os Invasores. Disponível em: https://www.youtube.com/watch?v=0Zxt7kS5miQ - acessado em 22/10/2018

Para complementar o que conversamos até aqui, vamos assistir ao vídeo "Os Invasores", veja:

Existem também o Spam, nome dado aos e-mails indesejados que são enviados em massa, automaticamente, por empresas ou pessoas, a fim de divulgar uma empresa ou um serviço.

Podem ser fonte de invasões também, porque os trojans são frequentemente enviados por Spam.

Os Spams, além de causar perda de tempo, geram um aumento de tráfego desnecessário nas redes de comunicação. Frequentemente possuem conteúdos impróprios, podem provocar erros na rede e outros tipos de problemas.

Antispam.br – 3/4 – Spam. Disponível em: https://www.youtube.com/watch?v=DFL5TbyfhrU - acessado em 22/10/2018.

Para se proteger dos spams, ative o AntiSpam da sua caixa de correio eletrônico, não forneça o seu e-mail a sites que não considere confiáveis, crie filtros para os seus e-mails e não clique em links suspeitos de e-mails ou páginas de internet.
Para conhecer melhor sobre o spam, assista ao vídeo AntiSpam.br – 3/4 que demonstra os diversos problemas que podem ser causados pelas mensagens não solicitadas.

O **Ransomware** surgiu como outra modalidade de ataque. Esse malware torna os dados do equipamento atacado inacessíveis, geralmente com a utilização de criptografia dos dados. Para reaver o acesso às informações é exigido o pagamento de um resgate em criptomoedas.
Um computador pode ser infectado por um Ransomware ao se clicar em links que instalam programas contendo um código malicioso ou por meio de vulnerabilidades de sistema como quando uma empresa inteira foi infectada via rede.
Quando um computador é infectado por um ransomware raramente se tem acesso aos dados novamente, a não ser que você ou sua empresa tenha uma cópia de segurança (backup) dos dados.

Saiba mais sobre Ransomware? Acesse "O que é ransomware?". Link: https://www.infowester.com/ransomware.php - acessado em 22/10/2018.

Outra grande preocupação que devemos ter atualmente são as extensões ou plugins que utilizamos em nossos navegadores de internet. É inegável que eles aumentam muito a nossa produtividade e facilitam a vida no nosso cotidiano nos poupando tempo e aborrecimentos. Contudo, quando adicionamos uma extensão ao nosso navegador, em geral, ela tem acesso a todas as informações que acessamos ou digitamos, inclusive o acesso a dados sigilosos. Por esse motivo devemos ter muito cuidado ao instalarmos tais plugins e ter a certeza de que podemos confiar no seu desenvolvedor.

Nunca se deve instalar extensões que não são adquiridas das lojas oficiais dos desenvolvedores dos browsers, porque essas extensões não são verificadas quanto a presença de malwares.

As mesmas informações apresentadas aqui para as extensões dos navegadores valem para os aplicativos de celular.

Assim como a tecnologia, as técnicas para os golpes na internet estão em constante evolução, portanto, temos que ter o máximo de cuidado ao navegar por essa grande rede.
Aqui foram apresentados alguns malwares, mas existem também outros tipos de golpes como a clonagem de páginas de bancos e de grandes empresas e comércios eletrônicos para a obtenção de dados, páginas de vendas falsas etc., portanto desconfie de ofertas mirabolantes, preços muito reduzidos ou qualquer outra coisa que fuja do comum.

Prevenção e proteção contra as ameaças virtuais

Como já foi dito anteriormente, as técnicas de tentativas de golpes virtuais se aperfeiçoam a cada dia, assim como os métodos para tentar prevenir, combater e recuperar os danos causados pelos criminosos.

É um clichê, mas a frase se aplica perfeitamente nesse caso: “É uma eterna briga de gato e rato” para quem trabalha com segurança da informação. Assim que um método de ataque é detectado e corrigido, os criminosos inventam outro tipo de ataque explorando novas vulnerabilidades até que essas brechas no sistema sejam corrigidas e o ciclo prossegue indefinidamente.

Imagem 04

Mas, então, como podemos nos prevenir? Seja no ambiente corporativo ou doméstico, sempre, mas sempre, devemos focar no usuário. Ele é a peça fundamental da segurança de um sistema, seja ele um computador, uma rede, um celular ou tablet.

Deve-se instruir a pessoa que utiliza um computador a não adotar um comportamento de risco, e segurar o seu impulso de curiosidade, principalmente quando nos deparamos com links ou ofertas suspeitas ao navegarmos pela internet ou aplicativos de trocas de mensagens.

Para tanto, numa empresa, deve-se assegurar que os empregados tenham conhecimento da sua Política de Segurança.

Veja algumas soluções mais adotadas para combateras ameaças virtuais:

Imagem 05 vidadesuporte.com.br

1. Invista comportamentos preventivos dos usuários:

Oriente os usuários a não clicar em links estranhos recebidos por e-mails ou em páginas suspeitas na internet, por mais tentadores que sejam. Esse comportamento já previne grande parte das dores de cabeça por infecções cibernéticas

2. Caso tenha dúvidas da autenticidade de uma mensagem, confirme com o remetente antes de abrir qualquer link ou arquivo em anexo.

Muitos vírus e worms se utilizam da lista de contato dos usuários para se propagar com maior efetividade, uma vez que a tendência de clicar em algum link ou arquivo é maior se a mensagem for proveniente de alguém conhecido ou tido como “remetente confiável”.

3. Invista em um bom antivírus.

Existem excelentes antivírus gratuitos no mercado, assim como dezenas de produtos pagos.

4. Instale um programa de firewall.

Assim como os antivírus, existem soluções gratuitas e pagas. Um firewall tem a função de tentar impedir ataques pela rede de computadores. Pode-se considerar também a utilização de uma solução integrada de antivírus mais firewall conhecidas como “Internet Security” que facilitam a utilização por todos as funcionalidades estarem agrupadas em um único programa.

5. Sempre mantenha os seus programas atualizados.

Os desenvolvedores de software estão constantemente atualizando os seus programas com novas funcionalidades e principalmente corrigindo falhas e vulnerabilidades detectadas após o lançamento. Sabemos que muitas vezes as atualizações, principalmente as automáticas, são inconvenientes pois deixam a nossa “internet lenta” enquanto estão realizando o update, algumas pedem a reinicialização do computador, entre outros incômodos, mas na medida do possível, sempre mantenha os seus programas atualizados, principalmente o Sistema Operacional e os programas de antivírus e firewall.

6. Utilize senhas de acesso complexas.

Senhas são uma grande fonte de dor de cabeça para a maioria das pessoas, principalmente quando nos esquecemos delas. Contudo, devemos evitar a utilização de senhas fáceis como datas de nascimento, números de documentos pessoais, telefones, nomes de parentes, e palavras presentes em dicionário.

Palavras de dicionário são todas as que estão presentes em um dicionário comum e que podem facilmente ser utilizadas automaticamente para uma tentativa de acesso não autorizado por um programa malicioso como, por exemplo, deus, administrador, amor, senha.

Para criarmos senhas fortes e seguras devemos utilizar letras minúsculas e maiúsculas, números e caracteres especiais (quando o sistema permite a utilização destes). Elas também não podem ser curtas com menos de oito caracteres.

Mas como decorar uma senha dessas? Uma dica: pense em uma frase com pelo menos oito palavras e pegue a primeira letra de cada palavra como a senha. Por exemplo: Hoje eu vou estudar muito sobre segurança digital. A senha poderá ser: H3v3mssd. Obs.: a letra “e” foi trocada pelo número “3”.

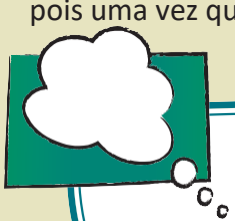
Não custa lembrar: jamais passe a sua senha para ninguém, nem anote em um papel.

7. Troque as suas senhas periodicamente e não utilize a mesma para serviços diferentes.

O tempo recomendado para a troca das senhas é de três em três meses, principalmente se forem senhas de instituições financeiras

8. Evite o compartilhamento desnecessário de informações pessoais.

Não publique em redes sociais informações sobre onde mora, telefones de contatos, seus hábitos cotidianos, pois uma vez que essas informações caem na internet é impossível controlar a disseminação delas.



Dica: nunca publique informações pessoais na internet ou em redes sociais que você não diria a um estranho que acabou de conhecer a alguma pessoa que não seja de confiança na vida real.

9. Utilize sites de compras conhecidos na internet.

Desconfie de ofertas mirabolantes que aparecem na internet. Realize compras somente em sites renomados ou após realizar uma pesquisa em órgãos de defesa do consumidor para saber se o site é idôneo. Se estiver na dúvida sobre a autenticidade da oferta de um site, digite o endereço do site manualmente na barra de endereços do navegador e procure pela oferta/produto ao invés de clicar na oferta recebida por um link. Muitos golpistas se utilizam de endereços quase idênticos ao site original com a diferença de um ponto ou uma letra que induza ao erro como por exemplo a letra “l” ele minúscula com a letra “I” i maiúscula.

10. Não utilize o armazenamento automático de senhas oferecidos pelos navegadores de internet ou sistemas operacionais.

Não use o auto salvamento de senhas porque se a senha do sistema operacional for descoberta, o invasor terá acesso a todos os serviços.

11. Não esqueça de sair do sistema.

Assim que acabar de utilizar o internet banking, realizar uma compra ou utilizar o e-mail, saia do sistema (logoff) para garantir que ninguém não autorizado tenha acesso as informações.

12. Cuidado com as crianças.

A internet é um paraíso para novas informações, vídeos etc. Porém, muita coisa ruim também está presente na rede. Oriente e supervisione o que as crianças e adolescentes fazem durante o uso da internet. Existem programas que restringem o acesso à internet e até podem monitorar o que os pequenos acessam na rede. Vale a pena investir na utilização destes.

13. Faça um backup dos dados regularmente.

Tenha o hábito de realizar a cópia de segurança dos seus dados regularmente, seja de modo manual ou automático, com a utilização de um programa próprio para backup.

14. Tenha bom senso.

Como já dito anteriormente, o bom senso das pessoas ao utilizar um dispositivo eletrônico é fundamental para a segurança das informações.

Adaptado de https://www.tecmundo.com.br/crime-virtual/97401-crime-virtual-proteger-ameacas.htm - acessado em 12/11/2018.

EXERCITANDO APRIMORANDO

E

6. Diferencie um vírus de um worm.
7. Como funciona um Ransomware?
8. O que faz um keylogger? E um screenlogger?
9. Por que uma simples extensão para um browser pode ser perigosa para a privacidade?
10. Como podemos nos prevenir de ameaças virtuais?

Respostas:

6. Um vírus é um programa de computador malicioso que realiza cópias de si mesmo infectando programas e arquivos. Ele depende que um programa ou arquivo seja executado pelo usuário. Já um worm pode fazer isso automaticamente enviando cópias de si mesmo pela rede explorando vulnerabilidades do sistema.

7. Um ransomware é um programa malicioso que criptografa algumas regiões do disco rígido ou até mesmo o HD inteiro e, geralmente, exige um resgate pago em criptomoedas para ter os dados restaurados.

8. Um keylogger é um software capaz de capturar tudo que digitamos no teclado de um dispositivo. Já um screenlogger tem a finalidade de capturar as telas do dispositivo.

9. Um simples complemento ou extensão para um browser pode ser perigoso pois este pode ter acesso e coletar tudo que realizamos durante a navegação pela internet. Por isso devemos sempre ler quais privilégios

essa extensão terá e sempre termos certeza de que a fonte e o desenvolvedor da extensão são confiáveis para evitarmos problemas de roubo de dados.

10. Algumas simples medidas já previnem muitas dores de cabeça quando o assunto são pragas virtuais. Podemos instalar antivírus, firewall, utilizarmos senhas complexas, não clicarmos em links suspeitos, desconfiar de promoções irreais, entre outros.