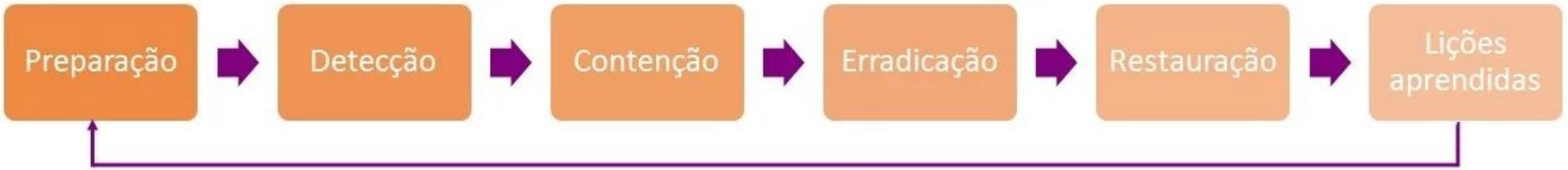
INE5429-07208
Segurança em Computação
IDS e IPS

Prof. Jean Everson Martina

Respostas a incidentes

- Respostas a incidentes é um conjunto de ações dentro dos serviços gerenciados de segurança que busca entender os incidentes.
- Quando executadas de forma eficaz, oferece um rico ciclo de aprendizado acerca do incidente (classificado como “casos desconhecidos” e “novos casos”)
- Mas vale ressaltar que muitas vão além da segurança em si, impactando e sendo impactadas por operações gerais da rede como:
    - arquitetura, gerenciamento de sistemas e até mesmo help desk e suporte local.

Ciclo de Respostas a Incidentes



Preparação

- A primeira etapa de um incidente realmente vem antes do início do ataque.
- Com a implementação de novos sistemas de detecção, com a criação de procedimentos específicos e com a atualização dos diversos sistemas utilizados.
- A compreensão do funcionamento dos sistemas e atividades de rede também é considerada parte da preparação

Detecção

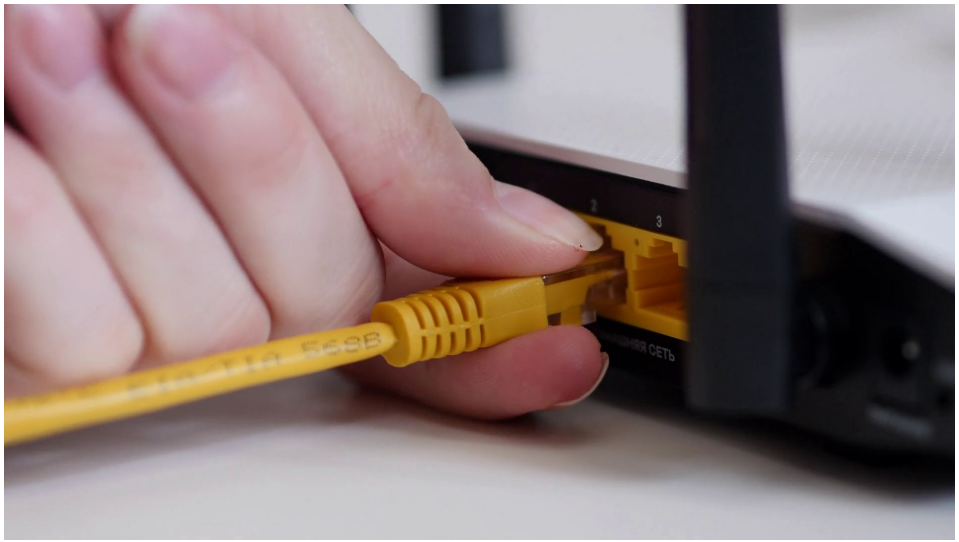
- A fase de detecção é o momento em que a equipe identifica a presença de um atacante
- Isso pode ocorrer de diversas formas:
  - identificando o invasor que consegue o acesso à rede, monitorando o tráfego, etc.
- Qualquer que seja a forma como ela ocorre, a fase de identificação começa quando se toma conhecimento do ataque.
- Esta fase normalmente leva à fase de investigação sobre o ataque e o atacante, antes de começar o processo de resposta.

Detecção

- Um dos principais objetivos da inteligência de ameaças é incrementar a fase de identificação para coletar o máximo de informações possíveis sobre o atacante
- Isso enriquece o processo, trazendo mais assertividade e aumentando a quantidade de métodos utilizados para identificá-lo rapidamente em futuras tentativas.

Contenção

- Aqui começa a fase da resposta real de bloqueio do ataque.
- A contenção é a tentativa inicial de mitigar as ações do atacante, interrompendo-as no curto prazo enquanto se prepara a resposta de longo prazo.
- Essas respostas de curto prazo não tornam o ataque impossível, mas reduzem drasticamente as chances de sucesso.

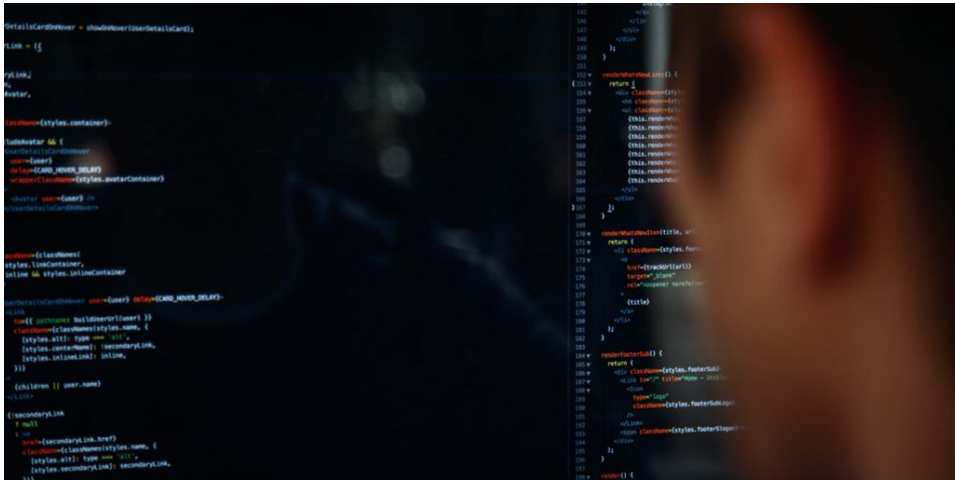


Contenção

- Estas ações devem ser tomadas de forma rápida, mas controlada.
- A contenção pode incluir a desativação da porta do switch à qual um determinado sistema está conectado ou mesmo bloquear temporariamente uma conta de usuário sob o controle de um intruso.

Erradicação

- A erradicação consiste nos esforços de mitigação a longo prazo destinados a manter o atacante do lado de fora da rede.
- Estas ações devem ser bem pensadas e podem levar uma quantidade considerável de tempo e recursos a serem implantados.
- Agora é o momento de eliminar completamente o ataque, remover definitivamente o malware e rever contas de usuários e mecanismos de persistência utilizados pelo intruso.



Restauração

- A restauração é o processo de voltar o sistema para o estado inicial, ou seja, sem as consequências do incidente.
- Esta fase depende das duas anteriores e, geralmente, existe a necessidade que ocorra uma coordenação com outras equipes, como administradores e engenharia de redes.
- Restauração requer a remoção de malware dos sistemas, redefinição de credenciais (como logins, senhas e certificados), atualização de softwares e outras mudanças ajustadas para remover a presença do atacante, limitando sua capacidade de retorno.

Lições Aprendidas

- A última fase do ciclo consiste em avaliar as decisões tomadas, aprender com elas e melhorar ações futuras.
- Nesta fase avalia-se o desempenho da equipe em cada etapa.
- Basicamente isso leva ao relatório do incidente e responde algumas perguntas básicas que devem ser utilizadas para todas as etapas no novo ciclo

Perguntas Genéricas Relevantes:

- O que aconteceu?
- O que fizemos bem?
- O que poderíamos ter feito melhor?
- O que faremos diferente na próxima vez?
- Qual o objetivo do atacante?
- Qual o meu descuido no processo?
- Foi falha de processo ou falha de operação?
- De quem são as responsabilidades?

Perguntas Especificas Relevantes:

- Preparação
  - Como poderíamos evitar o incidente?
    - Isso inclui mudanças na sua arquitetura de rede, configuração do sistema, treinamento dos usuários e criação ou modificação das políticas internas.
  - Quais políticas ou ferramentas poderiam ter melhorado todo o processo?
- Identificação
  - Que fontes de telemetria (IDS, fluxo líquido, DNS, etc.) poderiam ter facilitado o processo ou seriam mais rápidas para identificar esse ataque?
  - Que assinaturas ou inteligência de ameaças poderiam ter ajudado?

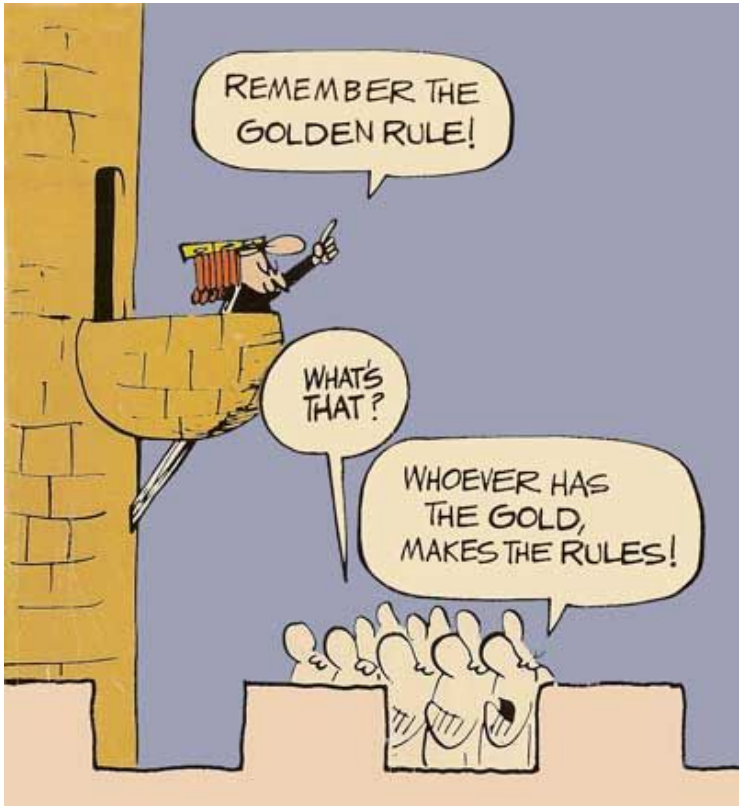
Perguntas Especificas Relevantes:

"Good news. The test results show it's a metaphor."

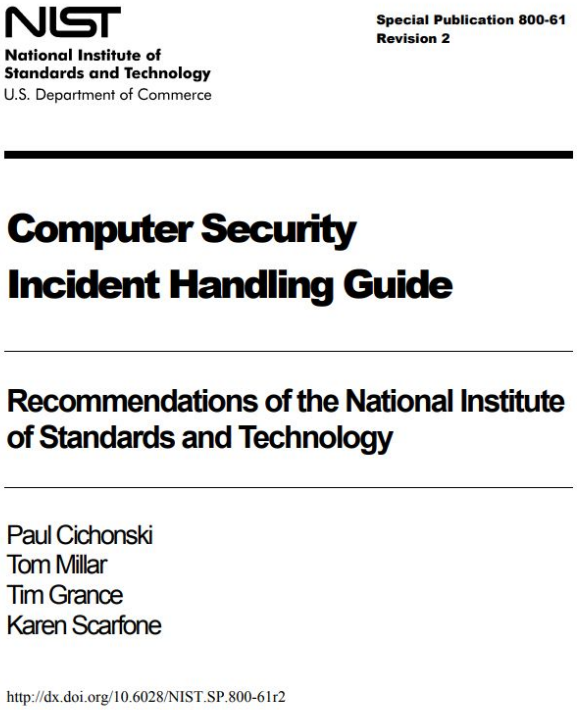
- Contenção
  - Que medidas de contenção foram eficazes?
  - Quais não foram?
- Erradicação
  - Quais etapas de erradicação foram bem realizadas?
  - O que poderia ter sido feito melhor?
- Recuperação
  - O que retardou a recuperação?

Regra de Ouro

- A prioridade de tratamento de um incidente deve ser definida de acordo com o impacto gerado aos negócios.
- A indisponibilidade de sistemas gera custos diretos ou indiretos e, principalmente, credibilidade perante acionistas e clientes.
- Segurança depende de otimização do custo versus o benefício



Onde estudar isso mais a fundo:



NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-61
Revision 2

Computer Security Incident Handling Guide

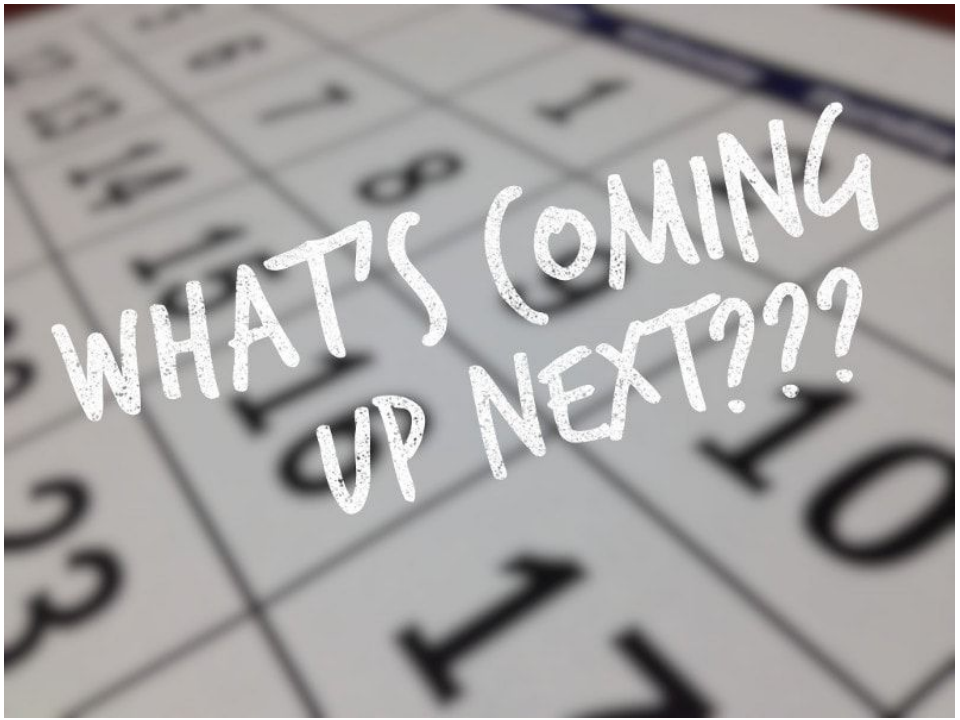
Recommendations of the National Institute of Standards and Technology

Paul Cichonski
Tom Millar
Tim Grance
Karen Scarfone

http://dx.doi.org/10.6028/NIST.SP.800-61r2

Próximas Aulas

- Prática:
  - Trabalho Individual V
    - Envolve todo este conteúdo que vimos na aula de hoje e o que veremos nas próximas.
  - Próxima Aula Teorica:
    - Aspectos Legais e Éticos



Perguntas?

jean.martina@ufsc.br