SEGURANÇA EM ARMAZENAMENTO, TRATAMENTO E CONSUMO DE DADOS

PUC Minas Virtual

PUC Minas
Virtual

UNIDADE IV – SEGURANÇA DOS DADOS

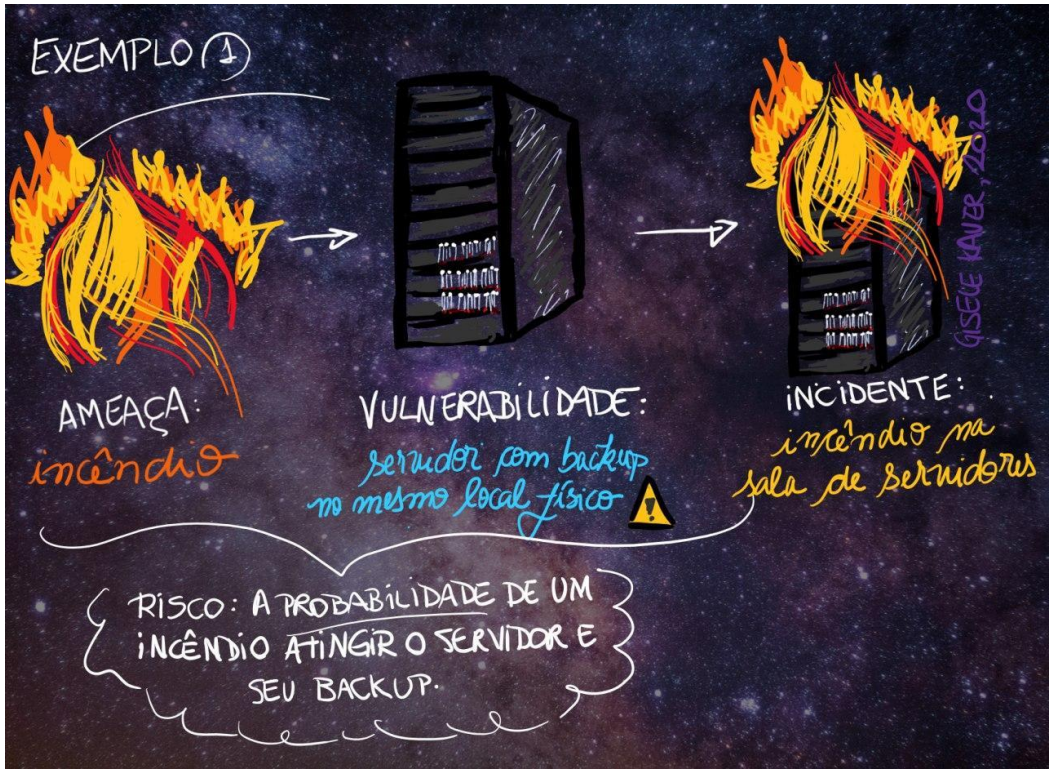
PUC Minas
Virtual

4.3 – FERRAMENTAS E TÉCNICAS PARA APONTAMENTO DE INCIDENTES DE SEGURANÇA

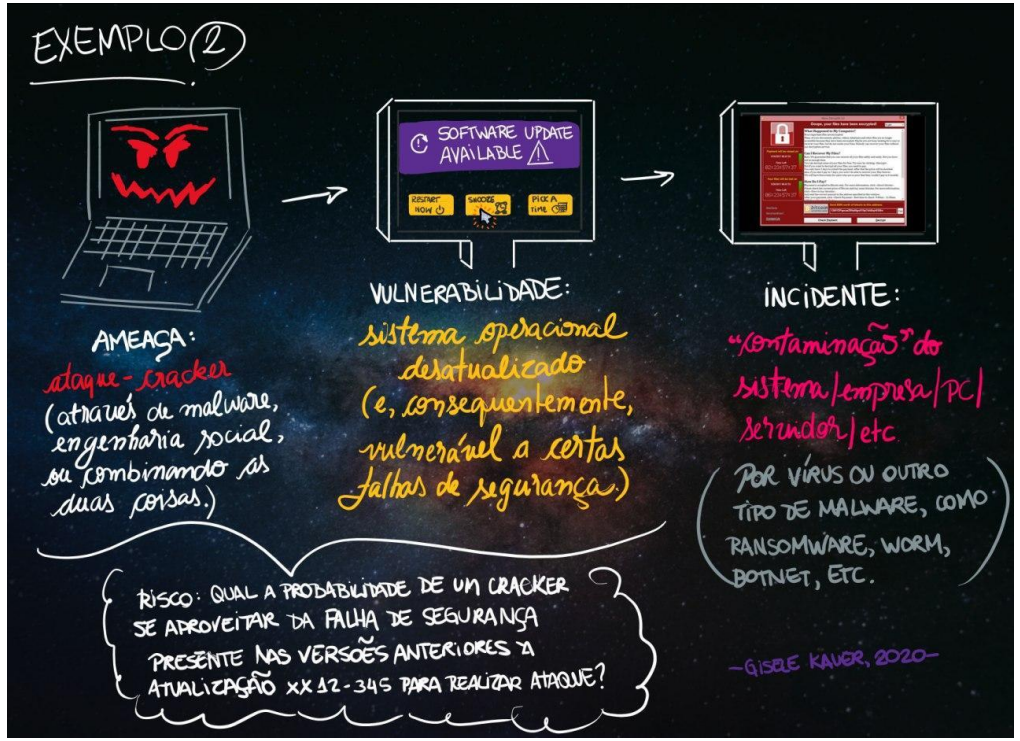
E SE DEPOIS DE TUDO ISTO?

Fonte: KAUER, 2020

E SE DEPOIS DE TUDO ISTO?



Fonte: KAUER, 2020



Fonte: KAUER, 2020

INCIDENTES DE SEGURANÇA

- Se acontecer o processo deve estar definido e deve ser de conhecimento de todos os participantes do fluxo.

- Mas relembrando: , um incidente de segurança é qualquer evento adverso, confirmado ou sob suspeita, relacionado à violação na segurança cibernética definida na empresa.

Qual o principal artefato no tratamento?

- **Plano de resposta a incidentes de segurança** um documento orientativo interno, que conduzirá as ações necessárias e imediatas caso aconteça um incidente de segurança na organização.
- Deve conter no mínimo: **1)** A definição de incidente de segurança; **2)** Descrição dos procedimentos a serem executados quando um incidente ocorrer; **3)** As ferramentas, tecnologias e recursos a serem utilizados em caso de incidentes e; **4)** Descrição dos colaboradores que fazem parte do processo e quais são suas responsabilidades e ações.

ATENÇÃO NA CLASSIFICAÇÃO

- **É necessário** traçar linhas nítidas sobre o que constitui ataques, que fazem com que sejam classificados como incidentes de segurança e não sejam chamados apenas de “incidentes”, em vez do termo mais alarmante que é “ataque”.
- Para que você consiga estabelecer de forma clara estes limites a sugestão passa pelas seguintes ações:

FERRAMENTAS PARA APOIO

Registrar e estabelecer as baselines de tráfego de dados para cada natureza de dispositivo.

Utilizar-se de Sistemas de Detecção de Intrusão (IDS) estabelecendo a forma de envio e recebimento de notificações dos eventos detectados;

Utilizar plataformas de detecção e resposta de endpoint (EDR) novidade que surgiu na ultima década para monitorar comportamentos fora do padrão em equipamentos de usuário final.

Utilizar o software antivírus é uma ferramenta de monitoramento que pode ajudar a detectar ataques.

FINALIZANDO

- A segurança da informação é realmente uma das mais complexas disciplinas para estudo pois como vimos envolve muitas outras questões em seu arredor.

- Frameworks como o NIST e normas como ISO nos ajudam a orientar os trabalhos em nossas empresas que podem ser melhorados através de ciclos PDCA e melhoria contínua.

REFERENCIAS BIBLIOGRÁFICAS

LEBLANC Jonathan. MESSERSCHMIDT, Tim. Identity and Data Security for Web Development. O'Reilly, 2016.

KAUER, Gisele. LGPD e a segurança da informação 2020. Disponível em: <https://infranewstelecom.com.br/lgpd-e-a-seguranca-da-informacao/>. Acesso em: 18 Nov. 2022.

GT Ad Hoc DPOs das EFPCs, 2021. Incidentes de Segurança com Dados Pessoais Disponível em: <https://biblioteca.sophia.com.br/terminal/9147/acervo/detalhe/22599>. Acesso em: 18 Nov. 2022.


PUC Minas
Virtual

PUC Minas
Virtual

OBRIGADO POR ASSISTIREM A ESTE CURSO!