Marsh

Como atuar em caso de ataque de Ransomware a terceiro?

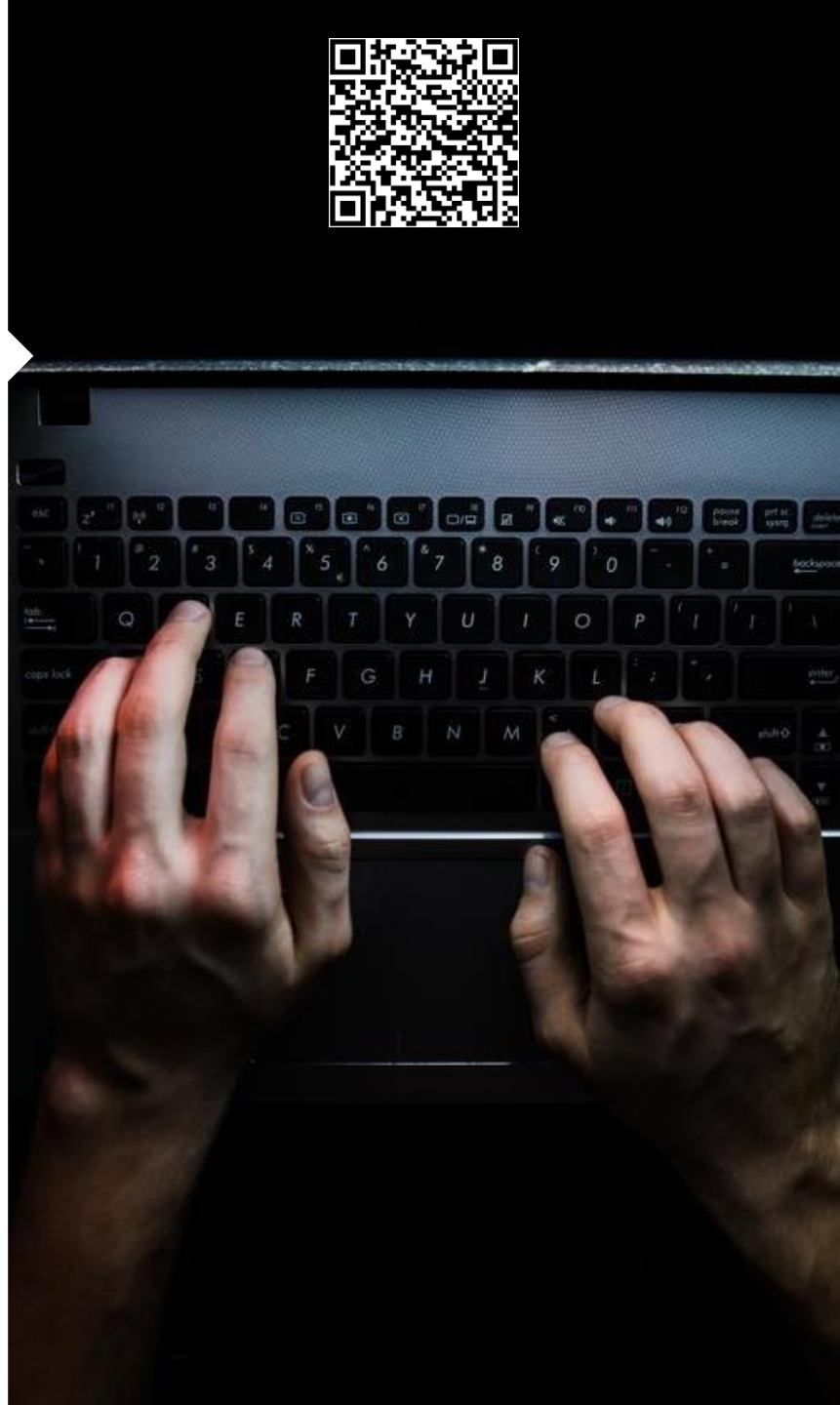
Recomendações Gerais

América Latina
2023

Cyber Risk Consulting
Marsh Advisory

O terceiro tem uma conexão direta através da rede ou de funcionarios locais?

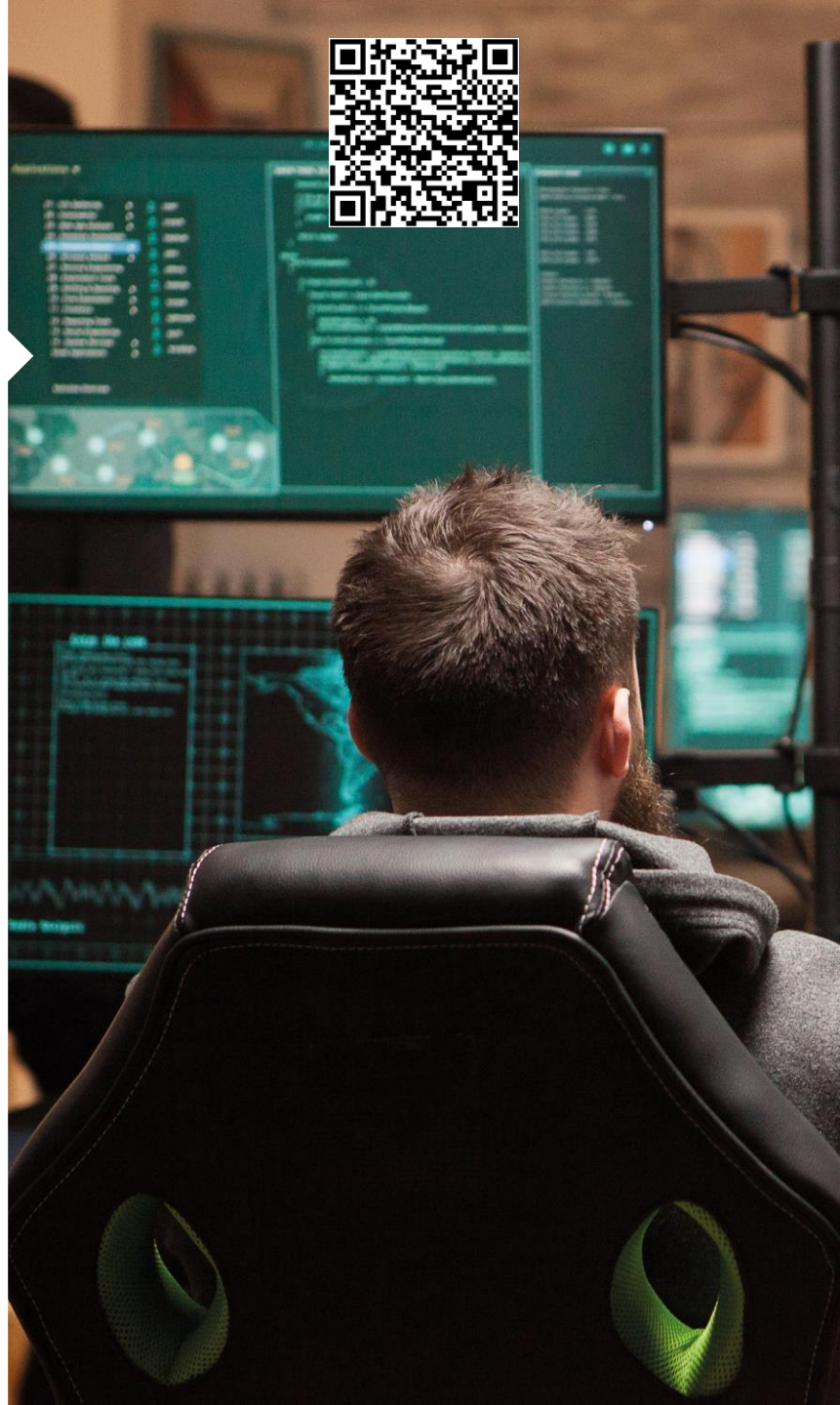
- Avaliar a possibilidade de acionar ou pelo menos avisar antecipadamente o Comité de Crise da organização e mantê-lo informado sobre a evolução da situação
- Avaliar a possibilidade de bloquear qualquer ponto de contato entre as redes e sistemas do terceiro afetado e a empresa (incluindo serviços de administração).
- Solicitar ou forçar o desligamento e desconexão de equipamentos de terceiros conectados à rede da empresa.
- Analise quaisquer padres suspeitos na rede que possam sugerir uma possível infecção:
  - Usuarios não reconhecidos.
  - Usuarios recem criados (principalmente com privilégios altos).
  - Tráfego de rede anormal (múltiplas conexões vindo principalmente das portas 139 e 445).
  - Grande volumen de dados saindo da rede nos últimos días, semanas ou meses.
  - Acesso a rede de localidades incomuns.
  - Conexões de rede para IPs hospedados em localidades incomuns.
  - Tentativas de conexão para e de IPs de reputação baixa.
  - Revisar os logs de auditoria de equipamentos e sistemas que não estão integrados às plataformas de monitoramento.
  - Solicite indicadores de comprometimento ao terceiro para validar se não há sinais de impacto na rede da organização.
  - Caso o terceiro possua credenciais da organização ou tenha acesso aos sistemas da empresa, avalie a possibilidade de forçar alterações de senha para evitar roubo de identidade.
  - Avaliar a possibilidade de enviar uma comunicação para aos colaboradores informando o ocorrido e solicitando para que reportem qualquer situação semelhante.
  - Analisar os contratos com clientes e terceiros que possam gerir descumprimentos e possíveis sanções.
  - Avaliar a possibilidade de exigir um relatório da situação, bem como as medidas implementadas para evitar que a situação se repita.
  - Se você possui seguro contra riscos cibernéticos, analise as coberturas que podem ser úteis em uma situação como a exposta.
  - Somente retome as conexões com terceiros depois de garantir, por meio de um relatório formal e que a ameaça foi erradicada e que a organização esta fora de perigo.
  - Após o incidente conduza uma sessão de lições aprendidas para entender o que funcionou e o que poderia ser melhorado em situações futuras.



Marsh

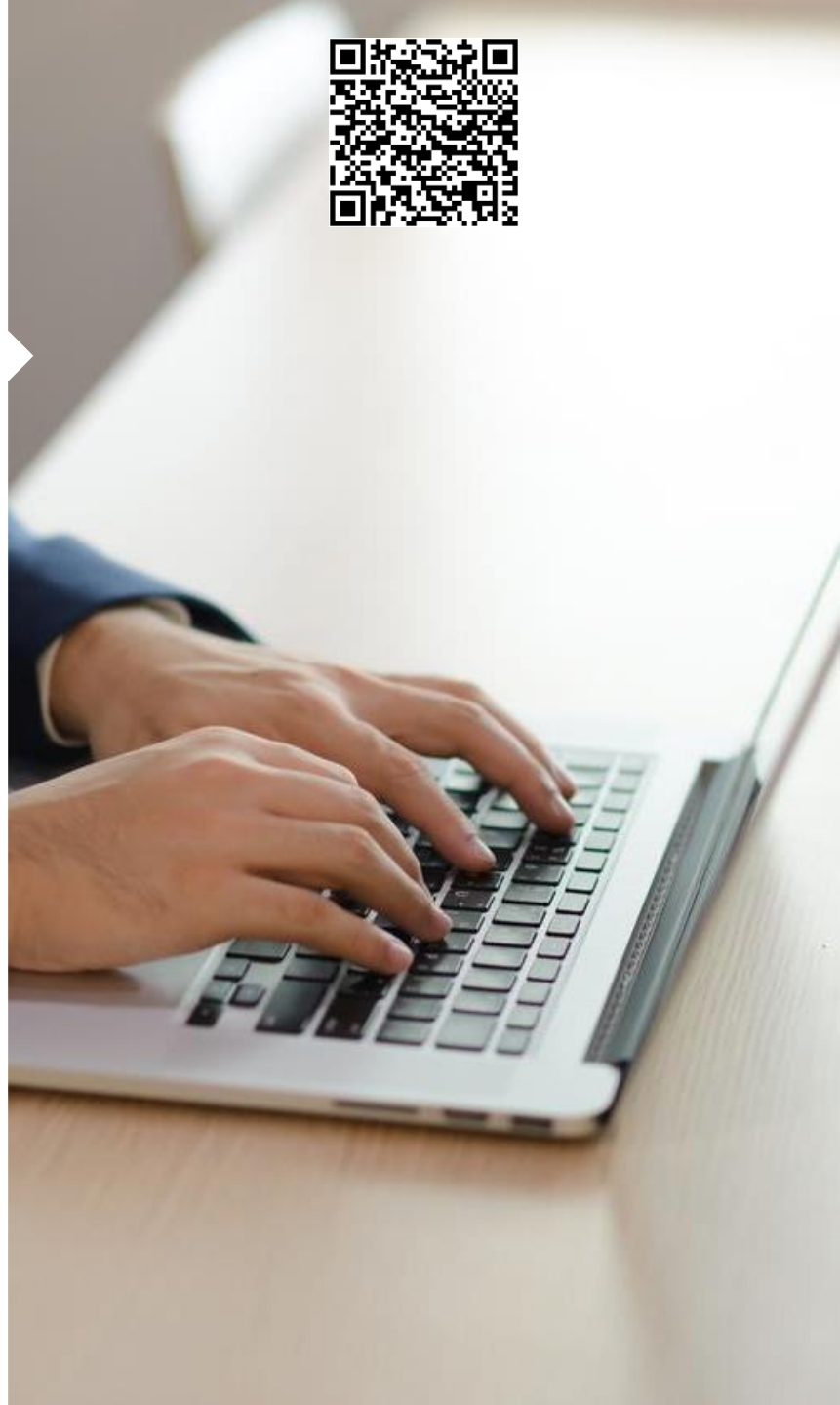
O terceiro armazena ou processa dados confidenciais da organização?

- Avaliar a possibilidade de acionar ou pelo menos avisar anticipadamente o Comité de Crise da organização e mantê-lo informado sobre a evolução da situação.
- Monitorar por meio de uma equipe especializada qualquer Informação exposta relacionada à organização.
- Caso seja confirmada a exposição ou acesso não autorizado do grupo criminoso a informações sensíveis da organização, faça o correspondente relatório ao reguladores e autoridades.
- Se a organização for uma entidade financeira e os dados dos clientes tiverem sido expostos, avalie a possibilidade de aumentar a sensibilidade do monitoramento de prevenção de fraudes para reduzir os casos de roubo de identidade.
- Avaliar a possibilidade de construção de mensagens base que serão enviadas às pessoas e empresas afetadas pela exposição dos dados de terceiros, de acordo com diferentes cenários relacionados à evolução do caso.
- Caso o terceiro possua credenciais da organização ou tenha acesso aos sistemas da empresa, avalie a possibilidade de forçar alterações de senha para evitar roubo de identidade.
- Na frente jurídica definir uma estratégia preventiva para atender possíveis reclamações que surjam devido ao impacto apresentado.
- Analizar contratos com clientes e terceiros que possam gerar descumprimentos e possíveis sanções.
- Avaliar a possibilidade de exigir um relatório da situação, bem como as medidas implementadas pelo terceiro para evitar que esta situação se repita.
- Se você possui seguro contra riscos cibernéticos, analise as coberturas que podem ser úteis em uma situação como a descrita.
- Ao final do incidente, conduza uma sessão de lições aprendidas para entender o que funcionou e o que poderia ser melhorado em situações futuras.



O envolvimento de terceiros gera interrupção nos procesos da organização?

- Avaliar a possibilidade de acionar ou pelo menos avisar antecipadamente o Comite de Crise da organização e mantê-lo informado sobre a evolução da situação.
- Avaliar a possibilidade de acionamento de planos de contingência que permitam manter os processos ativos, enquanto são recuperados da frente tecnológica. A recuperação pode levar horas, dias ou até semanas.
- Avaliar a possibilidade de construção de mensagens base que são enviadas aos stakeholders, de acordo com diferentes cenários relacionados à evolução do caso.
- Avalie a possibilidade de enviar uma comunicação aos colaboradores, com detalhamento de alto nível do ocorrido e para que eles relatem qualquer situação anormal. Além disso, solicite discrição e evite informações erradas.
- Caso o terceiro possua credenciais da organização ou tenha acesso aos sistemas da empresa, avalie a possibilidade de forçar alterações de senha para evitar roubo de identidade.
- Analisar contratos com clientes e terceiros que possam gerar descumprimentos e possíveis sanções em caso de interrupção prolongada.
- Se você possui seguro contra riscos cibernéticos, analise as coberturas que podem ser úteis em uma situação como a descrita.
- Ao final do incidente, conduza uma sessão de lições aprendidas para entender o que funcionou e o que poderia ser melhorado em situações futuras.



Marsh

Como a Marsh pode ajudar?

Consultoría de Segurança Cibernética

Principais Serviços

Ferramentas Especializadas

Estrategia e Governança

- Avaliação de segurança cibernética
- Desenvolvimento de Estratégia de Cibersegurança
- Avaliação de segurança cibernética ICS/SCADA
- Avaliação de segurança cibernética para nuvem
- Avaliação de prevenção de fraudes digitais
- Desenvolvimento de políticas e procedimentos de segurança da informação e cibersegurança
- Desenvolvimento do painel executivo de segurança cibernética
- Outsourcing de Segurança da Informação

Compliance

- Auditoria de controles gerais de TI
- Análise de lacunas de regulamentação de segurança cibernética
- Desenvolvimento de requisitos regulamentares de segurança cibernética
- Análise de lacunas do PCI DSS
- Desenvolvimento de Diagramas de Fluxo de Dados do Portador de Cartão (PCI DSS)
- Avaliação de privacidade de dados
- Implementação do Programa de Privacidade de Dados

Gestão e Quantificação de Riscos

- Identificação e Classificação de Ativos de Informação
- Desenvolvimento da Metodologia Qualitativa e Quantitativa de Segurança da Informação e Gestão de Riscos Cibernéticos
- Segurança da Informação e Avaliação de Riscos Cibernéticos
- Quantificação de risco cibernético (CyberXQ, Cyber RFO, Marsh Blue[i] Cyber)

Gestão de Riscos Cibernéticos

- Definição da estrutura de gerenciamento de risco cibernético de terceiros
- Segurança de informações de terceiros e avaliação de risco cibernético
- Cyber Due-Diligence para Fusões e Aquisições (M&A)

Desenvolvimento Seguro

- Desenvolvimento da Metodologia de Ciclo de Vida de Desenvolvimento Seguro
- Treinamento de Desenvolvimento Seguro
- Revisão do código-fonte (teste de segurança de aplicativo estático)

Segurança Ofensiva e Defensiva

- Cyber Inteligência (busca de informações vazadas na Internet)
- Gestão de Vulnerabilidade
- Revisão da configuração de segurança (hardening)
- Penetration Test (ethical hacking)
- Web & Mobile Application Hacking
- Testes de Engenharia Social
- Testes Red Team

Cyber Risk Analytics

Cultura de Segurança

- Química Cibernética - Avaliação da Cultura de Segurança Cibernética
- Desenvolvimento do Programa de Conscientização sobre Segurança Cibernética
- Treinamento de segurança cibernética
- Avaliação da capacidade da equipe de segurança cibernética*

Seguro Cibernético

- Autoavaliação de segurança cibernética para o seguro cibernético*
- Cyber IDEAL – Estimativa de perdas de risco cibernético (violação de privacidade, ransomware e perda de receita comercial)*
- Classificação de segurança cibernética (BitSight e SecurityScorecard)*
- Avaliação de risco de seguro cibernético
- Colocação de seguro cibernético*
- Reivindicações Cibernéticas e Orquestração de Crise

Gestão de Incidentes

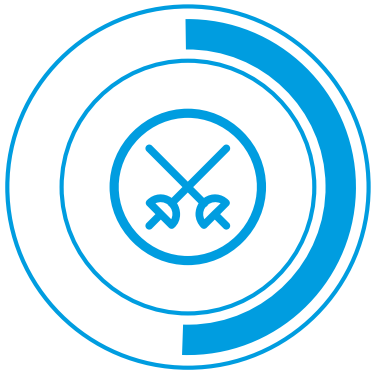
- Resposta a incidentes cibernéticos
- Desenvolvimento do Plano de Resposta a Incidentes Cibernéticos
- Desenvolvimento do Protocolo de Ransomware Organizacional
- Simulação de Crise Cibernética / Jogos de Guerra Cibernética
- Desenvolvimento do Plano de Melhoria Pós-incidente

Cyber Incident Management

Principais Serviços

PREVENÇÃO

- Avaliação das capacidades de resposta a incidentes.
- Desenvolvimento do Plano de Resposta a Incidente Cibernético e Playbooks.
- Desenvolvimento do protocolo de resposta organizacional contra ransomware.
- Desenvolvimento do plano de recuperação tecnológica em caso de ransomware.
- Treinamento de Gestão de Crises.
- Implementação do Cygnvs.
- Avaliação e remediação de risco de superficie de ataque (ASM).
- Cyber Threat Hunting.



PROVA

- Simulação de crise cibernética.
- Simulação de resposta a incidentes a nível tático/operacional.
- Testes de Red Team.

RESPOSTA

- Resposta a incidentes cibernéticos, incluindo:
  - Gestão de Crises.
  - Análise forense digital.
  - Ciberinteligencia.
  - Cyber Threat Hunting.
  - Entre outros.

POST

- Cyber Claims.
- Exercício de lições aprendidas.
- Cyber Threat Hunting.
- Implementação de melhorias.

Visite nosso centro De Recursos de Resposta a Incidentes Cibernéticos

A business of Marsh McLennan