OTRS Spotlight: Corporate Security 2024

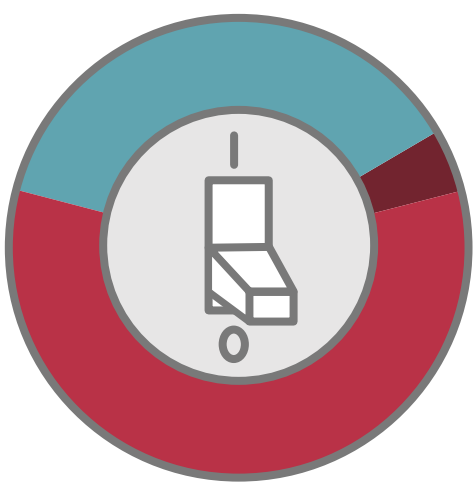
Parte 1: As Consequências do CrowdStrike

93%

Após o incidente da CrowdStrike, 93% das empresas pesquisadas aumentaram suas precauções de segurança.

- **45 %** Diversificamos nosso cenário de TI e software para sermos menos dependentes de um único fornecedor de software.
- **40 %** Implementamos sistemas avançados de monitoramento e alerta em tempo real.
- **39 %** Introduzimos testes adicionais para novos patches e atualizações.
- **39 %** Implementamos ou atualizamos nosso plano de resposta a incidentes.
- **36 %** Implementamos ou atualizamos nossos planos de recuperação de desastres e backup.
- **26 %** Mudamos para lançamentos em etapas/fases para patches e atualizações.
- **24 %** Implementamos o Unified Endpoint Management (UEM).
- **17 %** Desativamos as atualizações automáticas para todos os nossos sistemas.
- **4 %** Não tomamos nenhuma ação e **3 %** Não sei.

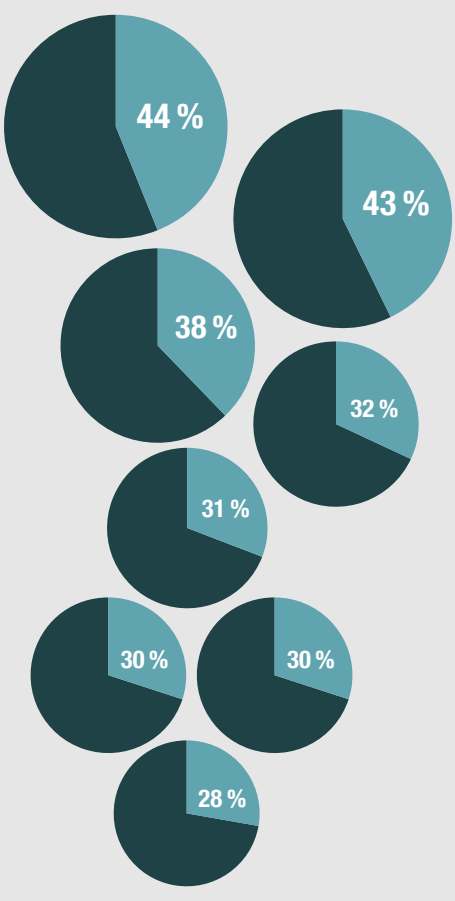
Embora nem todas as organizações tenham sido diretamente afetadas pelo incidente da CrowdStrike, foi um alerta para a maioria intensificar seu jogo de segurança de TI.



Algum dos sistemas da sua organização foi afetado pela interrupção de TI causada pela atualização defeituosa lançada pela CrowdStrike em julho de 2024?

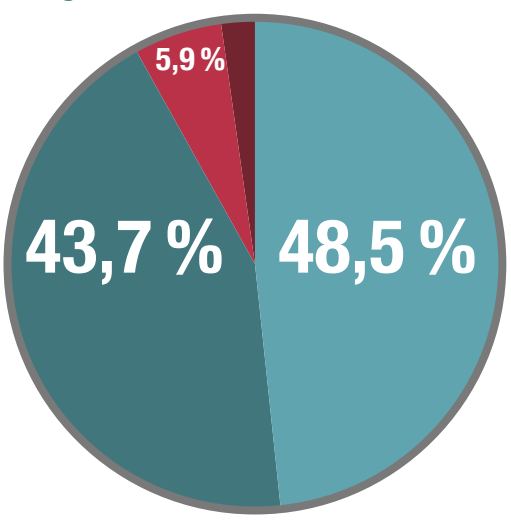
- **58,2 %** Sim.
- **37,4 %** Não.
- **4,4 %** Eu não sei.

Apenas alguns dos diretamente afetados estavam preparados para mitigar o impacto do incidente da CrowdStrike usando seus próprios recursos.



- **44 %** Seguimos as **etapas de correção descritas pela CrowdStrike** assim que elas estavam disponíveis.
- **43 %** Instalamos a **correção implantada pela CrowdStrike** assim que ela estava disponível.
- **38 %** Utilizamos **sistemas avançados de monitoramento e alerta em tempo real**, o que nos permitiu intervir rapidamente.
- **32 %** Temos **mecanismos robustos de reversão, recuperação de desastres e backups** em vigor, o que nos permitiu reverter rapidamente nossos sistemas para uma versão estável.
- **31 %** Usamos o **Unified Endpoint Management (UEM)**, que nos permitiu identificar rapidamente os sistemas afetados e iniciar as medidas apropriadas para mitigar o impacto (remotamente).
- **30 %** Temos um **plano robusto de resposta a incidentes** que nos ajudou a identificar, isolar e resolver rapidamente o problema.
- **30 %** Geralmente, fazemos **testes de pré-implantação para novos patches e atualizações**, o que nos permitiu detectar o defeito e intervir rapidamente.
- **28 %** Geralmente fazemos **implementações em etapas/fases**, o que significa que apenas alguns sistemas foram afetados pelo incidente.

Um banquete para os invasores: metade de todas as equipes de segurança não considera sua organização otimamente preparada para incidentes de segurança.



Quão bem-preparada está a sua empresa em caso de incidente de segurança?

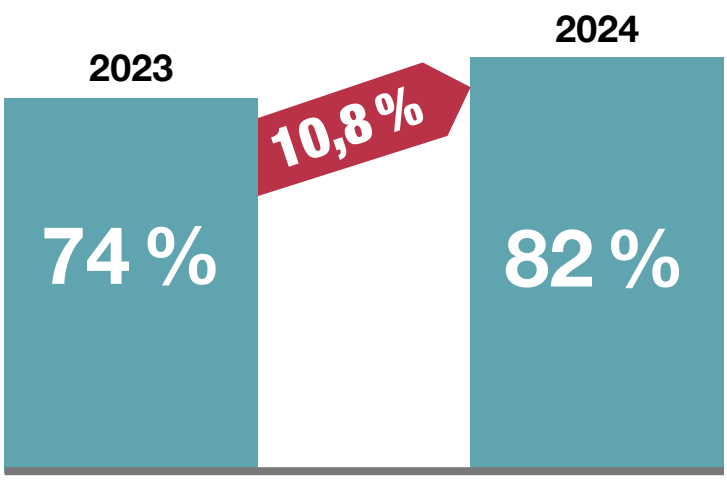
- **48,5 %** Otimamente.
- **43,7 %** Aceitavelmente.
- **5,9 %** Não o suficiente.
- **1,9 %** Não sei.

Os 5 principais desafios que as equipes de segurança enfrentam durante a resposta a incidentes:

34 % Ameaças em rápida evolução

- **15 %** Realização de revisões abrangentes pós-incidente
- **12 %** Falta de pessoal qualificado
- **12 %** Comunicação oportuna e apropriada com o público
- **12 %** Lacunas de comunicação entre ferramentas

O número de incidentes de segurança aumenta a cada ano, tornando difícil para as equipes de segurança acompanhar os invasores.



“Sim, temos visto um aumento nos incidentes de segurança.”

Ao automatizar seus processos de resposta a incidentes, as equipes de segurança têm mais chances de acompanhar as ameaças em rápida evolução.

Automação total
Automatizamos o máximo possível, com o mínimo de intervenção humana na resposta a incidentes.

Automação moderada
Automatizamos tarefas rotineiras, mas mantemos a supervisão humana para decisões críticas.

Automação limitada
Usamos automação básica para alertas, mas dependemos muito da tomada de decisão humana.

Sem automação
Contamos inteiramente com a intervenção humana para resposta a incidentes.

Os dados usados são baseados em uma pesquisa online realizada pela Pollfish Inc. em nome da OTRS AG, da qual participaram 476 profissionais de TI e segurança cibernética nos EUA, Alemanha, Brasil, México, Austrália e Malásia entre 22 de agosto e 17 de setembro de 2024. Salvo indicação em contrário, todos os valores referem-se à média de todos os países pesquisados.

OTRS