

Herstel na cyberaanvallen

Herstel activiteiten na een incident effectief en efficiënt.

Een uitgebreide beveiligingsstrategie voor herstel omvat

Het verzachten van de impact van de aanval



Het herbouwen van gecompromitteerde services en apparaten



Het herstellen van activiteiten



Het analyseren en leren van het incident

Stappen voor het verbeteren van cyberbeveiliging

1 Beheersing van incidenten
Sluit getroffen systemen af van het netwerk, schakel gecompromitteerde accounts uit en voorkom verdere schade.

2 Systeem-/ apparaat-herstel
Herbouw getroffen systemen, herinstalleer software en implementeer beveiligingspatches en -updates.

3 Dataherstel
Herstel data vanuit back-ups of gebruik gespecialiseerde technieken voor dataherstel om verloren of versleutelde bestanden terug te krijgen.

4 Forensische analyse
Onderzoek de mechanismen van de aanval en de gebruikte kwetsbaarheden om toekomstige incidenten te voorkomen.

5 Evaluatie van respons op incidenten
Evalueer het proces post-herstel om gebieden voor verbetering te identificeren.

6 Maak gebruik van AI/ML
Versnel herstel door getroffen systemen en data snel te identificeren en het herstelproces vanuit back-ups te automatiseren.

Cyberherstel is teamwerk.

Professionele services en partnerschappen
Cyberbeveiligingspartners bieden waardevolle expertise en middelen:

- Forensische analyse
- Identificatie van de oorzaak van de inbreuk
- Maatregelen om toekomstige incidenten te voorkomen

Lees meer over het implementeren van een uitgebreide strategie voor cyberbeveiliging.

[Ontdek het e-book](#) →