DELL Technologies

중단을 초래하는 사이버 인시던트에 대비하고 계십니까?

사이버 공격과 관련된 위험과 비용은 계속해서 증가하고 있으며, 랜섬웨어 공격은 회사 운영에 가장 큰 피해를 주는 공격 중 하나입니다. 몇 주 또는 몇 달까지도 이어지는 긴 기간 동안 비즈니스를 운영할 수 없다면 조직의 장기적 성공에 치명적일 수 있습니다.

복구는 매우 중요하며 정상 운영으로 되돌리는 작업은 굉장히 어렵습니다. 서버와 방대한 양의 데이터 및 애플리케이션을 복원하고, 가장 중요한 애플리케이션을 최대한 신속하게 온라인 상태로 전환하며 RTO(Recovery Time Objective)를 충족하기 위해서는 많은 노력이 필요합니다.

72%

모든 IT 보안과 위험 관리 요건을 충족하도록 하는 데 외부 도움이 필요하다고 보고한 회사 비율[5]

비즈니스 복귀에 필수적인 지원 제공

인시던트 대응 및 복구 서비스

Dell Technologies의 업계 공인 사이버 보안 전문가 팀이 모든 단계에서 도움을 드립니다. Dell Technologies의 대규모 글로벌 네트워크를 기반으로 신속하게 대응하여 위협을 제거하고, 비즈니스 운영을 가급적 중단을 최소화하며 빠르게 복원할 수 있습니다.

지속적으로 증가하는 사이버 위협의 결과는 치명적일 수 있습니다

매 11 초 사이버 또는 랜섬웨어 공격 발생 빈도[1]

16 일 랜섬웨어 공격을 받은 후 평균 다운타임[2]

75% 2025년까지 1회 이상의 공격이 발생할 조직의 비율[3]

이상 60% 악용된 취약성으로 인해 데이터 손상을 경험한 회사의 비율[4]

인시던트 대응 및 복구 서비스

Dell Technologies Services는 사이버 인시던트를 경험한 고객에게 복구를 지원한 검증된 실적을 보유하고 있습니다.

인시던트가 발생하면 어떻게 해야 할까요?

운영에 영향을 받는 경우 발생 가능한 상황:

- 이메일 작동이 중단됨
- 데이터에 액세스할 수 없음
- 멀웨어 발생
- 네트워크 작동이 중단됨
- Active Directory 작동이 중단됨
- 트랜잭션을 처리할 수 없음
- 금품을 요구받음

지원 요청

지원 요청

즉각적인 대응을 위해 전문가 팀이 대기하고 있으므로, 다음 연락처로 문의하시기만 하면 됩니다.

Incident.Recovery@dell.com

복구

IRR(Incident Response & Recovery) 팀

모든 단계에서 전문가의 지원 제공

전문가에게 믿고 맡기세요

폭넓은 분야에서 다양한 능력을 갖춘 업계 공인 사이버 보안 전문가로 구성된 전담 팀이 방대한 전문 지식과 모범 사례를 제공합니다.

어떤 상황에서든 필요한 지원을 제공합니다

발생한 상황이나 영향을 받은 대상에 관계없이 필요에 맞는 서비스를 제공합니다. 먼저 상황을 파악한 후 신속하게 복구할 수 있도록 최적의 리소스를 투입합니다.

수행 작업

공격이 방금 발생했든, 복구 작업을 이미 진행하는 중에 더 빠른 대응을 위해 지원이 필요하든 상관없이, 대기 중인 전문가가 다음 작업을 수행합니다.

- 문제 파악 후 적합한 리소스 투입
- 위협 제거 및 보안 위험 완화
- 비즈니스 애플리케이션을 인시던트 발생 전 운영으로 복구
- 직원들이 업무에 복귀하도록 워크스테이션 재배포
- 전문적인 데이터 포렌식 서비스 제공
- 보안 강화 지원

지원 요청

- 몇 분/시간 내에 통화하여 일반적으로 48시간 이내에 지원 팀을 현장에 배치
- 다양한 위치와 언어의 여러 작업 흐름으로 100개 이상의 리소스로 확장(필요에 따라 유연하게 조정 가능)
- 업계 공인 사이버 보안 전문가 지원, 대다수 10년 이상의 경험 보유
- Dell 및 타사 인프라스트럭처 및 엔드포인트 디바이스 전반에 걸친 전문 지식 제공
- 엣지, 클라우드, 법률, 보험 등에 대한 지식과 경험 지원
- 170개 이상의 시장에 글로벌 서비스 지원
- 기술 소비 및 가용 예산에 따라 IT 솔루션 비용을 조정하여 지출할 수 있도록 혁신적인 지불 솔루션 사용**

복구

- 위협 행위자 근절
- 빠르게 정상 운영으로 복귀
- 워크로드 증가로 인한 기존 IT 인력 보강
- 강화된 네트워크 환경 재구축
- 반복되는 사이버 공격을 방지하기 위한 보안 전략을 개발 및 구현하여 보안 태세 개선
- 모범 사례 교육 및 공유

자세한 내용은 Delltechnologies.com/incident-response-and-recovery를 참조하십시오.

** Payment solutions provided to qualified commercial customers by Dell Financial Services (DFS) or through Dell Technologies group companies and/or through Dell's authorized business partners (together with DFS "Dell"). Offers may not be available or may vary by country. Offers may be changed without notice and are subject to product availability, eligibility, credit approval and execution of documentation provided by and acceptable to Dell or Dell's authorized business partners. In Spain, services are provided by Dell Bank International d.a.c branch in Spain and in remainder of the EU by Dell Bank International d.a.c, trading as Dell Financial Services which is regulated by the Central Bank of Ireland. Dell Technologies, DellEMC and Dell logos are trademarks of Dell Inc.

[1] 2021년 예상치, Cybersecurity Ventures: https://cybersecurityventures.com
[2] Why Ransomware Costs Businesses Much More than Money, Forbes, 2021년 4월 30일, https://www.forbes.com/sites/forbestechcouncil/2021/04/30/why-ransomware-costs-businesses-much-more-than-money/?sh=469c541a71c6
[3] Detect, Protect, Recover: How Modern Backup Applications can protect you from ransomware, Nik Simpson, Gartner, 2021년 1월 6일, https://www.gartner.com/doc/reprints?id=1-258HHK51&ct=210217&st=sb
[4] Dell의 의뢰로 Forrester Consulting에서 작성한 Thought Leadership Paper, BIOS Security – The Next Frontier for Endpoint Protection, 2019년 6월
[5] Dell Technologies의 의뢰로 Forrester Consulting에서 실시한 연구, 2020년 12월