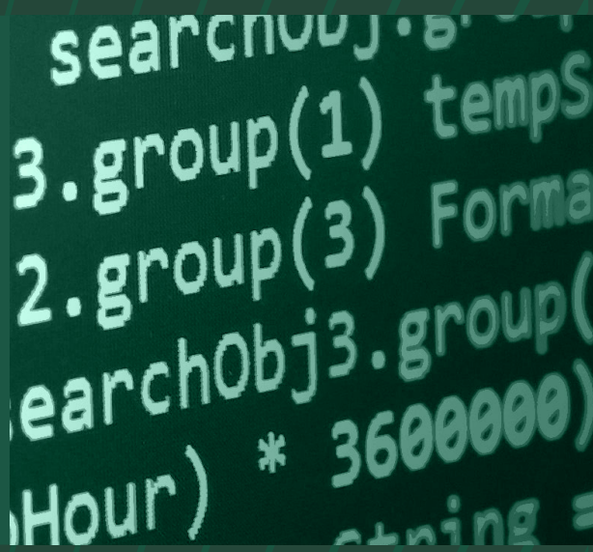
DELL Technologies

5 랜섬웨어 공격에서 벗어나기 위한 권장 사항



1 종합적인 인시던트 대응 계획 유지

공격의 영향을 최소화하는 데 집중

자주 연습, 테스트 및 업데이트

인시던트 대응 팀 사전 준비

사이버 보험을 전반적인 회복탄력성 전략의 일부로 고려

사법 기관과의 협력 계획 포함

2 명확한 커뮤니케이션 전략 수립

커뮤니케이션 템플릿 사전 작성

조직 내부에서 적시에 명확한 커뮤니케이션 보장

해당하는 경우 외부 커뮤니케이션 준비

관련 알림 규정 준수

3 강력한 데이터 보호 보장

격리되어 변경 불가능한 에어 갭 데이터 볼트(vault)에서 중요 데이터 보호

서비스/인프라스트럭처별 복구 우선순위 지정

복구 성능 연습

클린룸과 같은 기능을 RTO(Recovery Time Objective)에 페어링

복구 가능한 데이터의 무결성 보장

4 즉시 정상화된다고 가정하지 말 것

랜섬 비용 지불은 최후의 수단이 되어야 함

지불하기 전 법률 및 규제 요건 준수 보장

랜섬 비용을 지불하더라도 해커가 데이터를 돌려준다는 보장이 없음

5 훈련 및 교육 강조

공격 시뮬레이션 실시

직원의 보안 태세 관행 모니터링 및 테스트

피싱 테스트 및 이메일 보안 교육과 같은 툴 사용

더 이상 '공격 여부'의 문제가 아닌 '시기'의 문제입니다.

기업은 최선의 방어 수단에도 불구하고 공격을 피할 수 없다는 가정 아래 계획을 세워야 합니다. 재난이 발생했을 때 무엇을 해야 하는지 이야기하기 위해 Dell의 SME(Subject Matter Expert)이자 Cybersecurity and Compliance Practice 부문 Global Director인 Jim Shook 씨와 Cybersecurity Solutions and Strategic Partnerships 부문의 Principal Consultant인 Steven Granat 씨가 Dell Data Protection Product Marketing 부문의 Senior Consultant인 Brian White 씨와 만났습니다.

> 적절한 인재를 투입하여 훈련을 실시하고 행동을 시뮬레이션해야 공격이 발생했을 때 모든 사람이 무엇을 해야 하는지 바로 알 수 있습니다."
>
> **Steven Granat**, Principal Consultant,
> Dell Technologies Cybersecurity Solutions and Strategic Partnerships 부문

종합적인 인시던트 대응 계획 유지

공격이 발생할 때 조직의 모든 주요 이해 관계자는 물론 공급업체와 같은 제3자도 어떤 조치를 취해야 하는지 알고 있어야 합니다. 인시던트 대응 계획은 서면으로 명확한 조치 순서를 기술해야 합니다. 포괄적인 계획은 즉각적인 조치부터 회복에 이르기까지 기술, 프로세스 및 커뮤니케이션 단계를 다룹니다. 디지털 커뮤니케이션이 제대로 이루어지지 않을 수 있으므로 서면 문서도 유지 관리해야 합니다. "말 그대로, 직접 책장으로 가서 서류를 가져올 수 있는 계획이 필요합니다."라고 Granat 씨는 말합니다.

명확한 커뮤니케이션 전략 수립

대부분의 조직은 주요 이해 관계자와 소통해야 하며, 대다수의 경우 규제 요건을 준수해야 합니다. 누구에게 언제, 어떤 순서로 통지할 것인지에 대한 체계적인 지침이 포함된 내부 및 외부 커뮤니케이션을 위한 다양한 템플릿을 만드십시오. 전화와 이메일 시스템이 다운되는 것에 대비하여 계획하십시오.

강력한 데이터 보호 전략 구현

랜섬웨어 공격을 통해 데이터를 복구할 때의 주요 목표는 랜섬 비용을 지불하지 않으면서도 데이터를 복원하고 고통을 최소화하면서 복구하는 것입니다. 강력한 데이터 보호 전략은 이러한 목표를 달성하는 데 핵심적인 부분이지만 기술과 프로세스가 모두 갖춰져야 합니다. "변경 불가능한 데이터 및 사이버 볼트를 사용하여 신뢰할 수 있거나 최소한 시스템을 복구할 수 있는 검증 지점으로 사용할 만큼 충분한 데이터를 저장하십시오."라고 Shook 씨는 조언합니다. 데이터가 보호되도록 하는 것이 첫 번째 단계입니다. 데이터를 복구할 인력과 프로세스도 준비해야 합니다. 타사 전문가가 도움을 줄 수도 있지만 그러기 위해서는 계획 단계부터 참여해야 합니다.

랜섬 비용을 지불하더라도 즉각적인 정상화를 가정하지 말 것

최후의 수단으로만 고려해야 하는 랜섬 비용을 지불한다고 해서 즉시 정상화된다는 보장은 없습니다. 범죄자와 협상하는 것이라는 사실을 잊지 말아야 하며, 디코더 키를 받은 경우에도 새로 복구된 데이터를 위한 전략을 마련해야 합니다. 먼저 해독된 데이터를 테스트하고 모든 시스템을 체계적으로 재구축해야 합니다. 공격이 발생하기 전부터 여러 가지 가상 시나리오를 세심히 살펴보는 것이 회복탄력성을 높이는 데 큰 도움이 될 것입니다. "기술 인프라스트럭처의 다양한 응용 방식과 종속성을 이해하는 것은 효율적으로 안정화하는 데 매우 중요합니다. '사용 가능한 복구 소스와 복구 가능한 타겟이 있는가', '손상으로부터 자유로운 데이터가 있는가' 등이 중요한 고려 사항입니다."라고 Granat 씨는 말합니다.

복구 단계에서는 공격자가 실제로 시스템에서 나갔는지를 확인해야 합니다. "불이 완전히 꺼졌는지 확인하고 최초의 발화 지점을 파악해야 합니다. 이 두 가지 중요한 정보가 없으면 미래의 공격에도 계속 취약해지기 때문입니다."라고 Shook 씨는 말합니다.

훈련과 연습이 매우 중요

사이버 회복탄력성을 갖추기 위해서는 직원들이 강력한 사이버 보안 태세를 갖추도록 하는 것부터 복구 계획을 정기적으로 실천하는 것까지 포괄하는 종합적인 교육이 필요합니다. "적절한 인재를 투입하여 훈련을 실시하고 행동을 시뮬레이션해야 공격이 발생했을 때 모든 사람이 무엇을 해야 하는지 바로 알 수 있습니다."라고 Shook 씨는 말합니다.

오늘날의 위협 환경에서 랜섬웨어로 인한 피해는 불가피할 수 있지만, 계획과 실행을 통해 운영, 재정, 평판에 미치는 영향을 최소화할 수는 있습니다. 목표는 최대한 빠르고 원활하게 정상으로 돌아가는 것입니다.

dell.com/cybersecuritymonth에서 오늘날의 주요 사이버 보안 과제를 해결하는 방법을 알아보십시오.

DELL Technologies