The CannonDesign Ransomware Attack & How MDR Can Prevent Business-Disrupting Cyber Threats

March 26, 2025

The Incident: Ransomware Strikes a Leading Architectural Firm w/ 1,500 Employees

In January 2023, CannonDesign, a globally recognized architectural and engineering firm, was hit by a major ransomware attack by the Avos Locker group. The attackers exfiltrated 5.7 terabytes of sensitive corporate and client data, which included project schematics, IT infrastructure details, and personal employee information.

Following unsuccessful ransom negotiations, a second cybercriminal group, Dunghill Leaks, publicly leaked 2 terabytes of this data—exposing critical business information and causing long-term reputational and financial damage.

Cybersecurity Challenges for Architectural & Engineering Firms

Firms in the architecture, engineering, and construction (AEC) industry face unique cybersecurity risks due to their reliance on large-scale digital collaboration, sensitive intellectual property, and globally distributed project teams. Common challenges include:

- **Valuable Intellectual Property (IP):** Design blueprints, proprietary engineering solutions, and construction plans are lucrative targets for cybercriminals and competitors.
- **Extensive Third-Party Collaboration:** Shared access to project data across vendors, contractors, and cloud services increases the attack surface.
- **Legacy IT Systems & Software Gaps:** Many firms use a mix of outdated software and new digital tools, leaving vulnerabilities that hackers exploit.
- **Ransomware & Data Breaches:** With massive file storage needs, these firms are prime targets for ransomware attacks, which can halt operations and delay multimillion-dollar projects.

How MDR Services Can Prevent Business-Disrupting Cyber Attacks

CannonDesign's attack highlights the need for proactive cybersecurity measures. Implementing a Managed Detection and Response (MDR) service can significantly enhance an organization's ability to prevent, detect, and mitigate cyber threats before they cause irreversible damage. Here's how:

1. **24/7 Threat Monitoring & Rapid Detection** – MDR continuously monitors endpoints, networks, and cloud environments for suspicious activity, ensuring early threat detection before an attack escalates.
2. **Proactive Threat Hunting** – Advanced AI-driven analytics and expert security teams actively search for hidden threats within an organization's infrastructure.
3. **Rapid Incident Response & Containment** – MDR teams quickly contain and neutralize ransomware infections, minimizing data loss and downtime.
4. **Vulnerability & Risk Assessments** – By identifying weak points in an AEC firm's IT environment, MDR helps identify and patch vulnerabilities before attackers exploit them.
5. **Cloud & Third-Party Security** – With firms relying on cloud-based design tools (AutoCAD, BIM 360, Revit, etc.), MDR ensures secure access controls and real-time monitoring of file activity.

Strengthening Cyber Resilience in the AEC Industry

The CannonDesign ransomware attack serves as a wake-up call for architecture and engineering firms. Implementing MDR is no longer optional — it's essential to protect sensitive data, ensure project continuity, and maintain client trust.

Is your organization secure? Contact Blackswan Cybersecurity discuss, or take our free vulnerability assessment to better understand your current security posture and stay one step ahead of cybercriminals.

References

1. https://www.techradar.com/pro/security/top-architectural-firm-reveals-it-was-hit-by-major-ransomware-attack
2. https://www.bleepingcomputer.com/news/security/cannondesign-confirms-avos-locker-ransomware-data-breach/
3. https://www.scworld.com/brief/avoslocker-ransomware-attack-against-cannondesign-confirmed