Security Incident Management in Microsoft Dynamics 365

Published: April 26, 2017

This document describes how Microsoft handles security incidents in Microsoft Dynamics 365

© 2017 Microsoft Corporation. All rights reserved. This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it. Some examples are for illustration only and are fictitious. No real association is intended or inferred. This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

Introduction

Microsoft works continuously to provide highly-secure, enterprise-grade services for Dynamics 365 customers. This document describes how Microsoft handles *security incidents* in Dynamics 365. A security incident refers to any unlawful access to customer data stored on Microsoft's equipment or in Microsoft's facilities, or unauthorized access to such equipment or facilities that has the potential to result in the loss, disclosure, or alteration of customer data. Microsoft's goals when responding to security incidents are to protect customer data and the Dynamics 365 services.

The Dynamics 365 Security team and various service teams work jointly and take the same approach to security incidents: Preparation; Detection and Analysis; Containment, Eradication, and Remediation; and Post-Incident Activity.

Microsoft Approach to Security Incident Management

Microsoft's approach to managing a security incident conforms to the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61, and Microsoft has several dedicated teams that work together to prevent, detect, and respond to security incidents. The teams discussed in this document are described in Table 1.

Team	Description
Corporate, External, and Legal Affairs	CELA provides legal and regulatory advice in the event of a suspected security incident.
Cyber Defense Operations Center	CDOC is a 24x7 state-of-the-art facility that brings together security response experts from across the company to help protect, detect, and respond to cyber threats in real-time.
Dynamics 365 Customer Experience Communications	Engineering team responsible for all customer communications regarding security and service incidents.
Dynamics 365 Security Incident Response	Partners with Dynamics 365 service teams to build the appropriate security incident management process and to drive any security incident response.
Microsoft Security Response Center	The MSRC identifies, monitors, resolves, and responds to security incidents and Microsoft software security vulnerabilities.
Microsoft Threat Intelligence Center	MSTIC provides current information about digital security threats against Microsoft infrastructure and assets, helps partner teams inside Microsoft prioritize mitigation and prevention effort action plans, and increases protection by adopting near real-time incident monitoring and detection.
Microsoft Trust teams	Provide guidance on regulatory requirements, compliance and privacy.
Partner Security teams	Partner security teams inside Microsoft provide key services or are responsible for key dependencies in Dynamics 365, such as the Azure Security Response team and CDOC.
Service teams	Engineering teams for Dynamics 365 services that are responsible for security-related policies and decisions for each service.

Table 1 - Teams involved in Microsoft's security incident response management

Response Management Process

The Dynamics 365 Security team and service teams work together and take the same approach to security incidents, which is based on the response management phases in NIST 800-61:

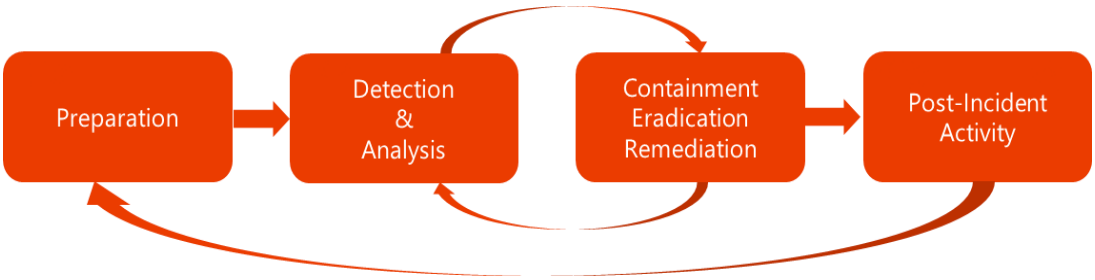

Figure 1 - NIST 800-61 Response Management Phases

Preparation

Preparation refers to the organizational preparation that is needed to be able to respond, including tools, processes, competencies, and readiness.

Training

Each employee working on Dynamics 365 is provided with training regarding security incidents and response procedures that are appropriate to their role. Every Dynamics 365 employee receives training upon joining, and annual refresher training every year thereafter. The training is designed to provide the employee with a basic understanding of Microsoft's approach to security so that upon completion of training, all employees understand:

- The definition of a security incident;
- The responsibility of all employees to report security incidents;
- How to escalate a potential security incident to Dynamics 365 Security Incident Response team;
- How the Dynamics 365 Security Incident Response team responds to security incidents;
- Special concerns regarding privacy, particularly customer privacy; and
- Where to find additional information about security and privacy, and escalation contacts.

Annually, the appropriate employees receive refresher training on security. The annual refresher training focuses on:

- Any changes made to Standard Operating Procedures in the preceding year;
- The responsibility of everyone to report security incidents, and how to do so; and
- Where to find additional information about security and privacy, and escalation contacts.

Moreover, each employee working on Dynamics 365 goes through an appropriate thorough background check that includes the candidate's education, employment, criminal history, and other specific information per United States regulations like HIPAA, ITAR, FedRAMP, and others. The background checks are mandatory for all employees working within Dynamics 365 engineering. Some Dynamics 365 environments and operator roles may also require full fingerprinting, citizenship requirements, and other more stringent controls. In addition, some service teams go through specialized security training.

Compliance Control

The Dynamics 365 Security team also develops guidance on compliance, security, and privacy based on the policies and procedures developed by CELA. All service teams use the Security team's guidance to setup the appropriate security and compliance controls inside of Dynamics 365.

Security Development Lifecycle

The Security Development Lifecycle (SDL) is a software development process that helps developers build more secure software and address security compliance requirements while reducing development costs. In January 2002, many Microsoft software development groups prompted "security pushes" to find ways to improve existing security code. Under this directive, the Trustworthy Computing (TwC) team at Microsoft formed the concepts underlying the SDL that has since continually evolved and improved.

Established as a mandatory policy in 2004, the SDL is an integral part of the software development process at Microsoft. The development, implementation, and constant improvement of the SDL represents a strategic investment in security. This was an evolution in the way that software is designed, developed, and tested, and it has matured into a well-defined methodology. Our commitment for a more secure and trustworthy computing ecosystem has also led to the creation of guidance papers, tools, and training resources that are available to the public.

Penetration Testing

Microsoft works with a variety of industry bodies and security experts to understand new threats and evolving trends. Microsoft continuously assesses its own systems for vulnerabilities, and contracts with a variety of independent, external experts who do the same. The tests carried out for service hardening within Dynamics 365 can be grouped into three general categories:

1. Automated security testing Internal and external personnel regularly scan the Dynamics 365 environment based on Microsoft SDL practices, Open Web Application Security Project (OWASP) Top 10 risks, and emerging threats reported by MTIC and different industry bodies.
2. Vulnerability assessments Formal engagements with independent, third-party testers regularly validate whether key logical controls are operating effectively to fulfill the service obligations of various regulatory bodies. The assessments are carried out by expert certified personnel and are based on OWASP Top 10 risks and other service-applicable threats. All found threats are tracked to closure.
3. Continuous system vulnerability testing Microsoft carries out regular testing in which teams attempt to breach the system using emerging threats, blended threats, and/or advanced persistent threats, while other teams attempt to block such attempts to breach.

Microsoft engages in ongoing wargames exercises and live-site penetration testing of our security and response plans with the intent of improving our detection and response capability. Microsoft regularly simulates real-world breaches, conducts continuous security monitoring, and practices security incident response to validate and improve the security of Dynamics 365 and other Microsoft cloud services.

Microsoft executes an assume breach security strategy using two core teams:

- Red Teams (attackers)
- Blue Teams (defenders)

Azure, Dynamics 365, and Office 365 staff have separate full-time red teams and blue teams. Referred to as *Red Teaming*, the approach is to test systems and operations using the same tactics, techniques, and procedures as real adversaries, against the live production infrastructure, without the foreknowledge of the infrastructure and platform engineering or operations teams. This tests security detection and response capabilities, and helps identify production vulnerabilities, configuration errors, invalid assumptions or other security issues in a

controlled manner. Every red team breach is followed by full disclosure between the red team and blue team to identify gaps, address findings and significantly improve breach response.

> Note: No customer data is deliberately targeted during Red Teaming or live site penetration exercises. The tests are against Dynamics 365 infrastructure and platforms, as well as Microsoft's own tenants, applications and data. Customer tenants, applications and data are never targeted.

Red Teams

The Red Team is a group of full-time staff within Microsoft that focuses on breaching Microsoft's infrastructure, platform, and Microsoft's own tenants and applications. They are the dedicated adversary (a group of ethical hackers) performing targeted and persistent attacks against online services (but not customer applications or data). They provide continuous "full spectrum" validation (e.g. technical controls, paper policy, human response, etc.) of service incident response capabilities.

Blue Teams

The Blue Team is comprised of a dedicated set of security responders, as well as members from across the security incident response, engineering, and operations teams. They are independent and operate separately from the Red Team. The Blue Team follows established security processes and uses the latest tools and technologies to detect and respond to attacks and penetration attempts. Just like real-world attacks, the Blue Team does not know when or how the Red Team's attacks will occur or what methods may be used. Their job whether it is a Red Team attack or an actual assault, is to detect and respond to all security incidents. For this reason, the Blue Team is continuously on-call and must react to Red Team breaches the same way they would for any other adversary.

Detection and Analysis

Detection and Analysis refers to the activity to detect a security incident in a production environment and to analyze all events to confirm the authenticity of the security incident. To detect malicious activity, Dynamics 365 centrally logs security events and other telemetry and performs various analytical processes to find anomalous or suspicious activity. Log files are collected from Dynamics 365 servers and infrastructure devices and stored in a central, consolidated database.

As developing step-by-step processes for handling every potential incident is impossible, Microsoft takes a risk-based approach to detecting malicious activity. We leverage incident data and threat intelligence to define and prioritize our detections.

Employing a team of highly-experienced, proficient, and skilled people is one of the most important pillars of success in the detection and analysis phase. Dynamics 365 employs multiple service teams, and those teams include employees with competencies on all components within the stack, including the network, routers and firewalls, load balancers, operating systems, and applications.

The security detection mechanisms in Dynamics 365 also include notification and alerts that are initiated by different sources. The Dynamics 365 Security Incident Response team is the key orchestrator of the security incident escalation process. This team receives all escalations and is responsible for analyzing and confirming the validity of the security incident.

One of the primary pillars of detection is notification:

- Each service team is responsible for logging any action or event inside the service based on recommendations from the Dynamics 365 Security team. All logs created by the different service teams are processed by a Security Information and Event Management (SIEM) solution with predefined security and detection rules that evolve based on the Dynamics 365 Security team's recommendation, and on information learned from previous security incidents, to determine if there is any suspicious or malicious activity.
- If a customer determines that a security incident is underway, they may open a support case with Microsoft, which is assigned to the Dynamics Operations Center (DOC) and turned into an escalation.

During the Escalation phase, and depending on the nature of the security incident, the Dynamics 365 Security Incident Response team may engage one or more subject matter experts from other internal teams, including CDOC, MSTIC, MSRC, CELA, Azure Security, Office 365 Security, Dynamics 365 engineering, and others.

Before any escalation to the Dynamics 365 Security Incident Response team occurs, the service team is responsible for determining and setting the severity level of the security incident based on defined criteria such as privacy impact, scope, number of affected tenants, region, service, details of the incident, and specific customer industry or market regulations.

Incident prioritization is determined by using distinct factors, including but not limited to the functional impact of the incident, the informational impact of the incident, and recoverability from the incident.

After receiving an escalation about a security incident, the Dynamics 365 Security team organizes a virtual team (v-team) comprised of members from Dynamics 365 Security Incident Response team, service teams and the Dynamics 365 Incident Communication team. The more complex part of this team's activities is to confirm the security incident and eliminate any false positives. The accuracy of information provided by the indicators determined in the Preparation phase is critical. By analyzing this information by category of vector attack, the v-team can determine if the security incident is a legitimate concern. At the beginning of the investigation, the Dynamics 365 Security Incident Response team records all information about the incident and updates during the incident lifecycle, which includes:

- A summary, which is a brief description of the incident and its potential impact
- The incident's severity and priority, which are derived by assessing the potential impact
- A list of all indicators which led to detection of the incident
- A list of any related incidents
- A list of all actions taken by the v-team
- All gathered evidence, which is also preserved for post-mortem analysis and future forensic investigations
- Recommended next steps and actions

The flow chart shown in Figure 2 details the Dynamics 365 Security Incident Response team's process from the beginning of an escalation to containment, eradication, and remediation.

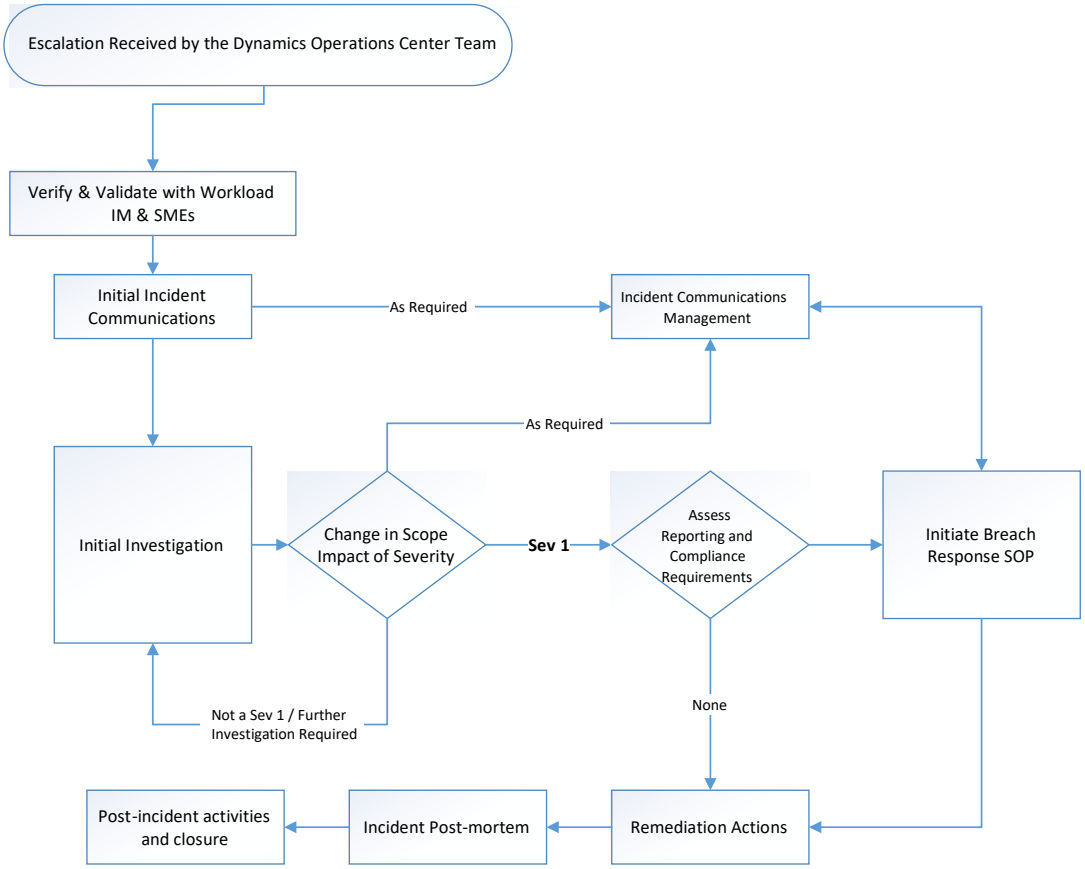

Figure 2 - Dynamics 365 Security Investigation and Response Incident Flow

After security incident confirmation, the primary goals are to contain the attack, to protect the service(s) under attack, and to avoid a greater global impact. At the same time, the appropriate engineering teams work to determine the root cause and to prepare the first remediation plan. In the next phase, the Dynamics 365 Security Incident Response team identifies the customer(s) affected by the security incident, if any. The scope of effect can take some time to determine, based on region, datacenter, service, server farm, server, and so forth. The list of affected customers is compiled by the service team and the Dynamics 365 CXP Communications team, who then handle the customer notification process.

Dynamics 365 service teams also use the intelligence gained in trend analysis through security monitoring and logging to detect abnormalities in Dynamics 365 information systems that might indicate an attack or a security incident. Dynamics 365 servers aggregate output from these logs in the production environment into a centralized logging server. From this centralized logging server, logs are examined to spot trends throughout the production environment. Data aggregated in the centralized server is securely transmitted into a logging service for advanced querying, dashboard building and detecting anomalous and malicious activity. The service also uses machine learning to detect anomalies with log output.

Containment, Eradication and Remediation

Containment, eradication, and remediation refers to the required and appropriate actions taken to contain the security incident based on the analysis performed in the previous phase. Additional analysis may also be necessary in this phase to fully remediate the security incident. Based on the analysis performed by the

Dynamics 365 Security Incident Response team, the service team, and others, an appropriate containment and remediation plan is developed to minimize the effect of the security incident. The appropriate service team(s) then applies that plan in production with support from the Dynamics 365 Security Incident Response team.

Using Microsoft Social Engagement (MSE) as an example, after receipt of a security event, or on the detection of anomalous behavior in MSE's production environment, a Dynamics 365 first responder triages the event, creates a ticket in Microsoft's internal issue tracking system and assigns it a priority. The responder also informs the MSRC about the case if the issue is declared a security incident.

From this point, the First Responder(s) must classify the event in one of two buckets:

- MSRC case A publicly reported security issue is escalated to the MSRC from the Microsoft Social Engagement First Responder. After escalation, an MSRC case number is assigned along with the appropriate severity, priority, and likelihood of authenticity. Dynamics 365 Security assesses and decides if the flaw is a known issue (in the process of addressing or has been addressed), or if it is a security vulnerability. Depending upon the severity, priority, and likelihood of authenticity, Dynamics 365 Security and MSRC will decide on an appropriate fix timeline.
- Software Security Incident Response Plan A software security incident is defined as an elevated risk to customer data due to software vulnerabilities. The response plan is the MSRC's plan of action to react, assess, and remedy these incidents.

Dynamics CXP Communications will also notify Microsoft executives and senior management during a software security incident and provide them with periodic updates. In addition, Dynamics 365 Security will notify security contacts from Microsoft Online Risk Management when there is a possible instance of unauthorized access or unauthorized use resulting in the loss, disclosure, or alteration of customer data.

Containment

After detecting a security incident, it is important to contain the intrusion before the adversary can access more resources or cause additional damage. Thus, the primary goal of our security incident response procedures is to limit impact to customers or their data, or to Microsoft systems, services and applications.

Eradication

Eradication is the process of eliminating the root cause of the security incident with a high degree of confidence. The goal is two-fold: to evict the adversary completely from the environment and (if known) to mitigate the vulnerability that enabled or could enable the adversary to re-enter the environment. Depending on the nature of the incident, the scope of the security incident, the depth of the penetration, and possible repercussions, the Dynamics 365 Security Incident Response team will recommend that service teams adopt eradication techniques. Considering the potential business impact that may be caused by these eradication steps, these decisions will be made by service teams and the Dynamics 365 Security Incident Response team after a detailed analysis and approval from the Executive Incident Manager, if necessary.

Recovery

As the response team gains a reasonable level of confidence that the adversary has been evicted from the environment and all known vulnerable paths have been eliminated, the individual service teams, in consultation with the Dynamics 365 Security Incident Response team, will initiate restoration steps to bring the service to a known and good configuration. This includes identifying the last known good state of the service, restoring from backups to this state, inspecting vulnerable attack paths in the restored state, etc. The Dynamics 365

Security Incident Response team, in consultation with the service teams, will determine the best possible recovery plan for the environment.

A key aspect to the recovery is to have enhanced vigilance and controls in place to validate that the recovery plan has been successfully executed, and that no signs of breach exist in the environment.

Notification of Security incident

If Microsoft determines that a security incident has occurred, we will notify you promptly. After identifying all affected tenants, the Dynamics 365 CXP Communications team works to identify any relevant regulations that might apply to affected tenants. The Dynamics 365 CXP Communications team uses the appropriate communication channel defined in applicable regulations to notify the appropriate tenant contact. Notification will include detailed information about the incident, such as a description of the incident, the effect on customer data, if any, actions taken by Microsoft, and/or suggested actions for customers to take to resolve the issue and prevent recurrence. Notification will be delivered to the designated administrator(s) of the Dynamics 365 tenant. To ensure notifications are received, you should ensure that your administrators provide and maintain accurate contact information in their tenant profiles.

Post-Incident Activity

Post-incident activities refer to the post-mortem analysis performed after remediation of a security incident. The operational actions performed during remediation are reviewed to determine if any changes need to be made in the Preparation or Detection & Analysis phases.

Post-mortem

After every security incident, the Dynamics 365 Security Incident Response team conducts a detailed post-mortem with all the parties involved in security incident response to list out the sequence of events that caused the incident, and to create a technical summary of the incident as supported by the evidence that includes the actors involved in the breach (if known), how the response was executed, and other key takeaways. The post-mortem is designed to identify technical lapses, procedural failures, manual errors, process flaws and communication glitches, and/or any previously unknown attack vectors that were identified during the security incident response. The post-mortem will directly influence Dynamics 365 service improvement, operational processes, and documentation by setting new priorities in the Dynamics 365 engineering development cycle.

Documentation

All key technical findings in post-mortems are captured in a report as well as service investments or fixes in the form of bugs or development change requests. These are then followed-up with the appropriate engineering teams. In the case of process failures and cross-organizational issues, issues are documented in the Dynamics 365 Security Incident Response team's database and followed-up with the appropriate groups to address them.

Process improvement

Responding to a security incident in Dynamics 365 involves coordination with multiple groups spread across different organizations within Microsoft, and potentially even appropriate external organizations such as law enforcement. We know that it is critical to evaluate our responses after every security incident for both sufficiency and completeness. In case of any identified improvements or changes, the Dynamics 365 Security Incident Response team evaluates the suggestions in consultation with the appropriate teams and stakeholders, and where appropriate incorporates them into standard operating procedures. All required changes, bugs or service improvements identified during the security incident response or post-mortem activity are logged and

tracked in an internal Dynamics 365 engineering database, and all potential bugs or features are assigned to an appropriate owner. The Dynamics 365 Security Incident Response team reviews all entries until the issue is resolved.

Summary

Microsoft works continuously to provide highly-secure, enterprise-grade services for Dynamics 365 customers. Our process for managing a security incident conforms to the approach prescribed in NIST 800-61, and we have several dedicated teams that work together to prevent, monitor, detect, and respond to security incidents. The Dynamics 365 Security team and the service teams work jointly and take the same approach as other Microsoft cloud services to security incidents, which include Preparation; Detection and Analysis; Containment, Eradication, and Remediation; and Post-Incident Activity.