Robust security in a crisis

Avanade Compromise Recovery can help you address the impact of the Solarwinds breach

avanade

Solarwinds and supply chain attacks: Where do you start?

There are two types of businesses – those who have suffered a compromise and those who don't know they have had a compromise.

As we have seen in recent news there is nothing that will keep a determined adversary out of your network. We need to evolve our cybersecurity posture with this in mind. From both a reactive and a proactive point of view, we must have the ability to report early and contain threats before they spread.

Patching doesn't preclude you from due diligence.

Avanade advises that you must follow proper protocol to ensure there are no known Indicators of Compromise (IOC's) in your environment. To do this you must have good visibility across endpoints, networks and your identity platform. If IOC's are found you must be able to contain, monitor for re-compromise, and reclaim your identity infrastructure if necessary.

The first 3 things you must do.

✓ Patch the known vulnerabilities immediately
✓ Gain 100% visibility into endpoints (EDR tool), networks (ingress, egress, lateral, DNS), authentication telemetry and monitoring
✓ Reclaim your networks and establish good confidence in your identity estate

Recover integrity and build resilience

Our goal is to bring your key stakeholders together with our security advisory experts to evaluate your current state, ensure awareness of key tactical measures to regain positive control and move forward with the vision of resilience. In working with our clients, we often see challenges around setting expectations during a cybersecurity incident. We recommend affording ourselves the opportunity to make decisions early that aren't meant to last; we refer to this as a *"Battlefield Mentality"* or 5-5-5.

First 5 Days

IDENTIFY AND CONTAIN

In the first 5 days we make decisions that last 5 weeks…

First 5 Weeks

STABILIZE AND CONTROL

Within the first 5 weeks we make decisions that last 5 months…

First 5 Months

REMEDIATE AND MANAGE

Within the first 5 months we make decisions that last 5 years…

A checklist of things you should do next:

- ✓ Ensure the backup/restore processes of your critical data and systems is where you want it to be
- ✓ Implement MFA where you can for critical systems and data (especially O365 and Azure)
- ✓ Isolate directory service (AD, Azure AD, etc.) administration using privileged admin workstations (PAW's)
- ✓ Rotate KRBTGT, federation tokens, and all Domain Admin, Enterprise Admin, schema and built-in admin credentials
- ✓ Block public internet ingress/egress and email for all high value privileged accounts
- ✓ Have a plan to rotate resources to keep your people fresh
- ✓ Continuous monitoring with incident IOCs for potential endpoint, credential, phishing, re-compromise
- ✓ Identification of "Patient 0," timeline establishment, containment of threat and modus operandi

Why Avanade?

We're the experts at helping you secure your Microsoft and hybrid IT ecosystems. Our security services provide a holistic approach through advisory, implementation and managed services. We are ready to assist throughout the incident lifecycle with our proven end-to-end playbook to restore integrity which extends from pre-incident, post-incident and future vision.

Proactive

We have an enhanced threat assessment to build confidence and readiness in your response processes and capabilities.

Tactical

Guiding your business through the tactical Incident Response (IR) and Compromise Recovery (CR) to ensure integrity and availability of critical data and systems.

Strategy

A robust strategy to bridge from the initial investigation and response of an incident to build on concepts of early warning and containment while moving towards resiliency.

Unparalleled expertise in securing the Microsoft platform

MICROSOFT SECURITY 20/20
SECURITY ADVISORY OF THE YEAR WINNER

GLOBAL ALLIANCE SI
MICROSOFT PARTNER OF THE YEAR 2020

#1 PARTNER MICROSOFT
SECURITY CERTIFICATIONS
AZ-500
MS-500

Member of
Microsoft Intelligent Security Association
Microsoft

avanade

About Avanade
Avanade is the leading provider of innovative digital and cloud services, business solutions and design-led experiences on the Microsoft ecosystem. With 38,000 professionals is 25 countries, we are the power behind the Accenture Microsoft Business Group, helping companies to engage customers, empower employees, optimize operations and transform products, leveraging the Microsoft platform. Majority owned by Accenture, Avanade was founded in 2000 by Accenture LLP and Microsoft Corporation. Learn more at www.avanade.com.

North America
Seattle
Phone +1 206 239 5600
America@avanade.com

South America
Sao Paulo
AvanadeBrasil@avanade.com

Asia-Pacific
Australia
Phone +61 2 9005 5900
AsiaPac@avanade.com

Europe
London
Phone +44 0 20 7025 1000
Europe@avanade.com