Makánal Tech

Case Study: "We've Been Hacked"

An SME discovers their network is compromised.

Overview

A consulting firm recently completes new construction of a satellite office—including a network installation performed by the ISP. A firewall misconfiguration and outdated firmware allows intruders to access the network. An employee makes a referral to bring in our team when the internet "stops working".

Profile

SME Platinum Client

Industry: Technology
Location: United States
Size: 25-50 Users

Company Bio
A satellite office of a large corporation recently constructed in a major U.S. city.

"It was bad, bad, bad before [Makánal Tech] cleaned up the mess."

- Partner
SME Platinum Client

The company had tech-aware employees but no trained IT professionals. The network was left wide open for bad actors who happened to discover it. And, of course, many did. Productivity was coming to a halt.

The Issue

Many SMEs do not have in-house IT personnel to configure, manage, and monitor the network. This particular firm moved in to a newly constructed office location. The ISP installed the network, and it all *looked* great. The rack gear was even locked away in a secure dedicated room with RFID entrance. The company had tech-aware employees but no trained IT professionals.

Within a couple months the network began crawling. An inexperienced—but willing—employee attempted to troubleshoot, making seemingly small adjustments. However, one of those adjustments disabled the network's firewall. The network was left wide open for bad actors who happened to discover it. And, of course, many did. Multiple intruders walked right through the network's open front door planting viruses, data miners, botnets, and rerouting all outbound traffic to multiple proxies. At least two intruders discovered the admin password on the primary router was saved in a plain text file on the network. They helped themselves to re-configuring network settings and creating new admin accounts that appeared to be genuine should the original password ever be changed.

Employees of the firm depend entirely on the internet to do their jobs. The majority of software and line-of-business systems are online, but users were barely able to get online. What's more, all outbound traffic was being routed through unrecognized proxies allowing bad actors to eavesdrop on network traffic. Even the RFID system was malfunctioning and preventing authorized employees from entering the office. Productivity was coming to a halt.

An employee knew one of our senior consultants and made the call. We knew we needed to work on-site to assess (and complete) the ISP's installation job, so we jumped on the next available flight.

The Approach

Our first task is always to stop the bleeding first. We wanted to enable the employees to get back to work as soon as possible. We knew we had to get into the network elements and track down—and remove—every point of intrusion and disruption. This type of troubleshooting and investigation can sometimes take technicians days on an unfamiliar network. But with Network Discovery, we had a real-time map of the physical network and a device inventory within a few minutes.

Once we had a visualization of the network and implemented proactive monitoring, we performed an Expert Network Assessment to identify root causes of issues and build a Remediation Action Plan.

Upon presenting the Remediation Action Plan to the site manager, we went to work executing it. We installed a best-practices firewall configuration and removed the discovered network vulnerabilities. We created new secure credentials for all network elements and disabled default logins. We installed missing hardware like an APC Smart-UPS with automatic voltage regulation instead of plugging critical network elements into wall sockets. We fixed the RFID security system so employees could enter the workplace with their badges. We reconfigured network printers to allow employees to print from their workstations. Finally, we cleaned up the cable nest entering the rack, created a photo inventory of the rack room, and did a little sweeping to remove the construction dust from the room.

"We were greeted with a long list of tasks ranging from installing critical hardware still in boxes to conducting network forensic analysis."

- Kane McConnell
Chief Managing Director

The Solution

As soon as we deployed our Network Discovery application, it immediately began mapping, cataloging, and examining every connected interface—physical and virtual. Network Discovery gives us a real-time "eye in the sky" over the whole network much like the military uses satellites to command and control operations.

Having this kind of visibility of the network allowed us to quickly conduct an Expert Network Assessment, which is like having a 100-point check performed on your car. We inspect every network element, device, interface, and service that is active on the network. We examine component configurations, credentials, and logs for vulnerabilities or misconfigurations. By the end of the assessment, we had a clear State of the Network, a Remediation Action Plan, and recommendations for future-proofing the network.

Once the company's network was restored to a secure and stable state, our SME Platinum Remote Managed Network service was the right-fit solution for the client. With SME Platinum Remote, we continue to provide:

- Active Monitoring 24/7/365
- Configuration Backups
- Quarterly Security Analysis
- Annual Hardware Review
- Preventative Maintenance
- Network Issue Remediation
- Quarterly CIO Consulting
- Unlimited Priority Support
- Quarterly Expert Network Assessment

The Results

Since our initial engagement and resolution of the issues, the client has experienced no further intrusion or capacity incidents. As an SME Platinum Remote client, we proactively monitor the client's network 24/7/365 from our network center.

We are very proud to manage a diverse, international portfolio of business technology and software development clients—including Fortune 500 companies. We are equally proud to be a Microsoft Partner and Amazon Technology Partner.

Our leadership team possesses an industry-diverse background allowing us to engage quickly with client projects that require practical industry experience as well as our technical expertise.

makanal.eu

Microsoft Partner