Nanitor

VERKÍS
VERKFRÆÐISTOFA

CASE STUDY

VERKIS

Verkís Consulting Engineers are the oldest consulting firm in Iceland that provides their premiere services in Iceland and abroad. Verkís provides consultancy for all areas of engineering and have managed projects like the Reykjanes Power Plant, the G.RUN Fish processing plant, and many other significant projects that required consulting services on many facets of the engineering services required to successfully complete these projects. In order to meet their customer's needs, Verkís IT infrastructure requires more than 400 devices that support their business objectives in various capacities.

The Verkís IT infrastructure can host information about their client's building schematics, data storage solutions, and other valuable information that attackers could sell or provide to their governments. Verkís provides consulting services to clients in different industries and could be a valuable target because of the range of information they host.

Verkís Security Obstacles

A primary business concern for Verkís, was that their IT infrastructure is an environment that depends on its availability to achieve their business goals. If their IT infrastructure becomes unavailable, it can hurt their relationship with customers and also cause financial damage (about 4-5 million IKR in salary cost, or $30,000 – $37,000 USD).
Verkís IT staff recognized that in order to guarantee availability, they'd have address their largest concerns when it came to cybersecurity:

01

No Overview on their Devices

Verkís did not have an overview of where their company stood when it came to cybersecurity. They utilized various tools to such as Microsoft's System Center Configuration Manager for software updates and local databases for asset management. They did not have a centralized view of their patch status and all the devices in their network.

02

Unaware of New Vulnerabilities

Verkís was only addressing vulnerabilities that were included in the patches and did not scan for any additional vulnerabilities. New vulnerabilities are discovered on a daily basis and although vendors regularly provide patches, that gap can provide attackers a window to exploit the vulnerability.

03

Prioritizing Identified Vulnerabilities

While Microsoft does provide the criticality associated with each patch, Verkís did not have enough information to prioritize which devices should be remediated first. Criticality of the vulnerability is one part of the equation; the other is addressing the assets that are the most important to your organization.

Leveraging Nanitor to Address Security Gaps

After a successful implementation of Nanitor in their environment, the Verkís IT staff recognized that Nanitor would help them protect their environment and address their primary concern which is availability. With the help of Nanitor's customer success team, Verkís has been able to prioritize the discovered issues, establish a technical policy and remediate the issues discovered. The customer success team has provided guidance during the remediation process by helping Verkis properly interpret the issues and implementing the recommended solutions provided in Nanitor.

Utilizing Nanitor's Issue Diamond

With the asset and issue RISC ratings that provide a prioritization score, Verkís has been able to focus their efforts on what will help protect the availability of their infrastructure. The remediation process has been streamlined by utilizing Nanitor's built in project feature that lets them track their remediation progress, assign issues, and automatically track any activity related to the issues within the project. All this is done without relying on any other tools.

Protecting NIX based devices

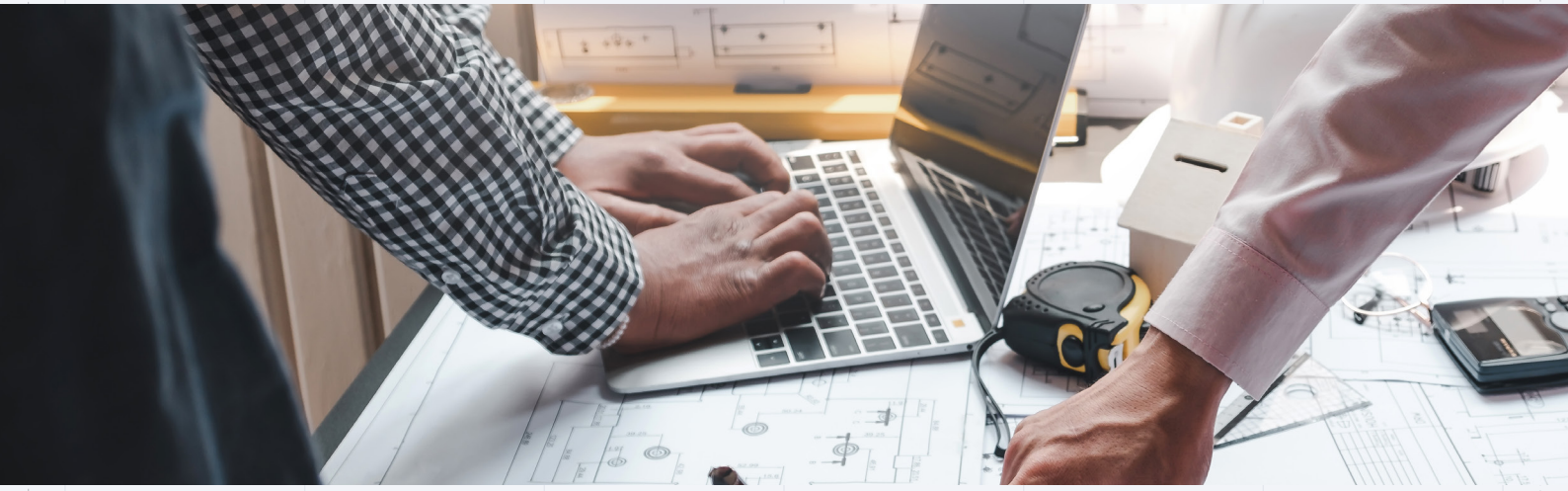
Previously Verkís had no consolidated view into the security state of any NIX based devices. Any patching or configuration management was not easily viewable but Nanitor provides them the ability to view these devices along with other Windows or network devices. They have the ability to know the security posture of the organization as whole, what exactly is on their network, view the specific vulnerabilities on any of their devices

Continuous Vulnerability Scanning

Verkís now continuously scans their IT environment with Nanitor's vulnerability scanner that receives daily updates from the National Vulnerability Database (NVD). Verkís has an accurate representation of their infrastructure and can make risk-based decisions when it comes to protecting their environment.

VERKÍS
VERKFRÆÐISTOFA

As Verkís continuous to mature their cybersecurity efforts, Nanitor has been valuable tool in providing them the necessary information to manage risk and incorporate security in their environment. With Verkís' continued desire for a secure IT environment and the assistance of Nanitor's customer success team, Verkís is on the path to hosting an environment that implements the latest cybersecurity practices that ensure the availability of their environment.



Nanitor

Nanitor is a powerful cybersecurity management platform focusing on hardening security fundamentals across your global IT infrastructure. The platform provides unique visibility and control of your security challenges that stakeholders can trust, at a fraction of the cost and time of alternatives.

Learn more at: www.nanitor.com
Email: sales@nanitor.com
+354 571 9080