

Minne Inno & MSP Business Journal: NetSPI adds ransomware attack simulation to its penetration testing portfolio

written by Aaron Shilts | June 29, 2021



On June 29, 2021, NetSPI President and CEO Aaron Shilts was featured in an article from Minne Inno and Minneapolis/St. Paul Business Journal:

Ransomware attacks have recently made headlines as everything from [meat suppliers](#) to [schools and hospitals](#) are falling prey to the unforgiving data breaches.

Minneapolis-based NetSPI, a network security firm, is now offering a [ransomware attack simulation service](#) to help companies protect themselves.

The service works by emulating real-world ransomware attacks to find and fix vulnerabilities in a companies cybersecurity defenses.

“The DNA and the way we deliver our work lends itself well to helping companies with ransomware,” said NetSPI CEO [Aaron Shilts](#).” ... We act as a ransomware attacker, using the same attacks, same tools and show them where their weakness would be.”

Shilts said the simulation not only illuminates where a breach can be made, but how the companies systems responded to the attack.

“That’s a big part of it. If you can detect something soon, you can usually protect it before they take out the entire network,” he said. “If you don’t have the detection capabilities, it will spread very quickly.

With tens of millions of dollars funneling towards the attackers, many of whom are backed by foreign governments, it seems like a daunting task to stay on pace with the attackers.

However, out of NetSPI’s 225 employees, 150 of them are cyber security experts that research and familiarize themselves with the latest attack patterns.

Shilts said the team is incredibly sharp and “lives and breathes” cybersecurity.

As far as who would benefit the most from the company’s service, Shilts said any operating business is a target to the attacks.

NetSPI’s work gravitates more towards heavily regulated financial services that store personally identifiable data. But less regulated industries such as K-12, state and local government are high targets because they’re easier to pick-off.

To learn more, read the full article here:
<https://www.bizjournals.com/twincities/inno/stories/news/2021/06/29/netspi-ransom-ware-attack-simulation.html>