READYING FOR A RISE IN SOFTWARE SUPPLY CHAIN ATTACKS

At a time when software supply chain attacks are at an all-time high, business leaders must deepen their IT knowledge and broaden their skills in software supply chain security. A Master of Information Technology degree from Virginia Tech prepares business leaders for the future.

When it comes to security breaches, organizations are often quick to point to nefarious actors. But increasingly, the source of an attack is a trusted software application or solution. That's because many of today's vendors unwittingly supply their customers with critical software that has been infected by malicious code.

Poorly developed software, deficient software update practices, and open source components can provide cybercriminals the opportunity to exploit weaknesses in a software supply chain. A software supply chain attack occurs when malicious code is intentionally inserted into a component, and then distributed to key targets along the supply chain.

With supply chain attacks increasing at an exponential rate of 4-5x per year, today's business leaders must understand the technology and deepen their competency in software supply chain management and security.

Virginia Tech's Master of Information Technology (VT-MIT) program provides working professionals the skills to identify vulnerabilities and understand risks to protect their software supply chain against imminent threats.

IN 2020, APPLICATIONS HAD AN AVERAGE OF 528 OPEN SOURCE COMPONENTS—AN INCREASE FROM 84 COMPONENTS PER APP IN 2016.

VULNERABILITIES EVERYWHERE

Over the years, open source components have allowed software capabilities to soar. In 2020, applications had an average of 528 open source components – an increase from 84 components per app in 2016, according to the 2021 Open Source Security and Risk Analysis report.

"Almost all software nowadays is third-party, open source code in some form or fashion," says Wade Baker, an associate professor of integrated security at Virginia Tech and VT-MIT faculty member.

With open source adoption comes a growth in vulnerabilities. As a result of anonymous contributors and unchecked quality assurance, a vulnerability can allow an attacker to gain access to an organization's IT environment. Worse yet, by infecting code in software that vendors supply to their customers, the attacker can unleash malicious code across a global supply chain.

In December 2020, SolarWinds fell victim to one such software supply chain attack. Malicious code was implanted into the company's Orion product. The attack enabled access to its network and application monitoring platform. Used by over 30,000 organizations, it cost the company at least $18 million in the first quarter of 2021, according to Reuters.

"Criminals know that software distributed to many customers is an excellent vector to spread an attack and quickly infect thousands of different organizations with malicious code," says Baker. "That's been a very attractive proposition to criminals, providing them with scale and reach while lowering the cost of launching an attack."

SPECIALIZE FOR A STRONGER DEFENSE

Specialized training can prepare today's leaders to become stewards of security. Virginia Tech's VT-MIT program allows students to specialize in pertinent, career-focused areas, such as software development and cybersecurity management.

"Students can take a selection of very targeted courses and come out well prepared to secure any organization's software supply chain," says Baker.

In cybersecurity management students learn the fundamentals of computer and network security, how to

- analyze a client-server IT infrastructure for security weaknesses, and
- implement security and trust controls for malicious behavior prevention, detection, and recovery.

Simultaneously, students may take specialized courses in software development to,

- deepen their understanding of the software lifecycle, and
- establish a foundation in the tools, techniques, and principles that underlie modern software development.

Together, these entirely customizable areas of specialization ensure professionals acquire the expertise needed to prevent a supply chain attack and mitigate its effects.

VIRGINIA TECH'S VT-MIT PROGRAM ALLOWS STUDENTS TO SPECIALIZE IN PERTINENT, CAREER-FOCUSED AREAS, SUCH AS SOFTWARE DEVELOPMENT AND CYBERSECURITY MANAGEMENT.

AN EDUCATION FOR THE FUTURE

Thanks to its highly customizable curriculum, U.S. News & World Report's Best Online Programs list for 2022 ranks the VT-MIT degree 3rd in the nation and 1st for veterans. In addition, the university carries the National Security Agency's designation for Center for Academic Excellence in Cyber Operations.

Whether enhancing existing skills or preparing for a major career transition, students will enhance their marketability with the VT-MIT cybersecurity management specialization. And, with more than 238,000 VT alumni from more than 100 countries, graduates can tap into an expansive network of professionals as they work to achieve their career aspirations.

Organizations will always make smart use of open source components to accelerate time-to-market of critical applications, free organizations from vendor lock-in, and reduce operational costs. Successfully securing the software supply chain demands a deeper understanding of cybersecurity risks and software development principles – an education made possible by a Virginia Tech Master of Information Technology degree.

Learn more about starting your VT-MIT degree from Virginia Tech **here**.