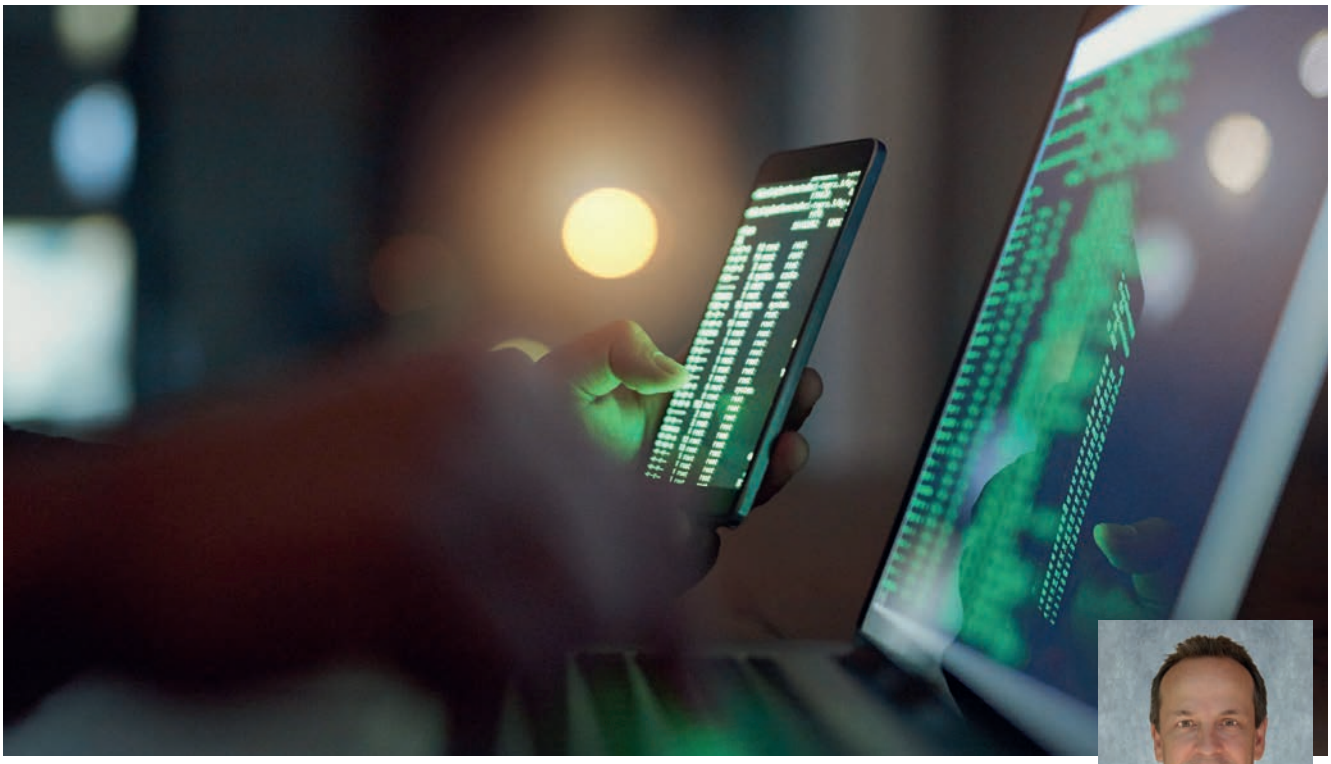

ATTACK PATH DISCOVERY

SUPPLY CHAIN SECURITY

Brent Whitfield, CEO, DCG Technical Solutions, California, USA

From Shanghai to Los Angeles, IT services and systems now connect the various infrastructures of the supply chain, creating a complex web of dependencies.

Each of these assets could theoretically become entry points for a cyberattack using known or new zero-day exploits.

In addition to patching vulnerabilities, cyber defense teams need to take a proactive stance by deploying intrusion detection systems (IDS) to actively sniff out potential threats.

SECURE SUPPLY CHAIN CHALLENGES

Our investment in cyber security has to match if not exceed that spent on physical security measures.

Intrusion detection is one of these measures.

It relies on accurately monitoring a network for signs of attack.

There is no one IDS able to monitor an entire supply chain, which means that each organization has a responsibility to investigate possible vulnerabilities in its networks.

This is a huge undertaking since attacks can come in from various local and global networks and affect multiple systems.

One of the first steps in securing a port from cyberattack is attack path discovery.

ATTACK PATH DISCOVERY

On one level, attack path discovery is, as the name suggests, the mapping of all possible routes and forms of cyberattack, from the local rogue employee seeking to sabotage operations to the international cybercrime syndicate looking to steal sensitive business data.

In reality, this process has to be parametrized.

Even in an age of distributed networks and cloud computing, there is not enough computing or human resources to monitor all possible attack vectors.

Therefore, attack path discovery is about mapping the most likely avenues of attack.

Attack path discovery uses an algorithm that searches system nodes for vulnerabilities, using known vulnerability lists.

An ideal attack path discovery program will yield the maximum useful information in the shortest amount of time while using the least amount of computer memory and processing power.

This is not an easy balance to strike.

One of the key decisions cyber security developers need to make involves how their algorithm will move from one node to another along a system tree.

A popular method is depth first search (DFS), a protocol whereby a branch is investigated to its maximum length before the program backtracks and checks other branches.

The strategy initially developed in the 19th Century as a way to efficiently calculate the optimal route through a maze.

It is not surprising that a similar method is calculating labyrinthine connections between IT systems in the supply chain.

DEPTH FIRST SEARCH DISCOVERY

DFS can quickly explore complex systems for vulnerabilities without using vast amounts of memory.

Unlike breadth first search, only the tree and the visited array need to be kept in memory to make this method potentially more efficient.

A disadvantage with DFS is that the

propagation length of the algorithm needs to be manually set to avoid the program heading off down one branch and never backtracking to map nodes closer to its starting point.

This, in effect, modifies the algorithm to become a depth limited search (DLS).

DFS also shares a disadvantage with all uninformed search algorithms in that every possibility will be checked until the vulnerability is found.

This is a fairly inefficient method when compared with informed searches which use a heuristic to choose which node to search next.

Models using informed searches are already being tested in the cyber security field and could lead the way to smarter attack path discovery algorithms in the future.

VALENCIA PORT CASE STUDY

An example of attack path discovery in action was demonstrated by the UK-based MITIGATE project, a European Union collaboration involving 12 partners with a scientific or industrial background in the maritime port domain.

MITIGATE used parametrized DFS search for attack path discovery along the Valencia port networks which made use of 26 different IT assets (through which vulnerabilities could be exploited).

Network administrators in control of the MITIGATE test could set a number of parameters to constrain the number of attack paths identified. These included:

- **Capability of the attacker:** This setting reflected the difference in network penetration that would be expected depending on the sophistication of the attacker or malware. There were three settings: low, medium and high. A low capability score would indicate a crude, opportunistic attack whereas a high capability score would mimic the impact of a sophisticated cybercriminal or piece of malware.
- **Location:** This parameter takes into account the different ways in which an attacker could seek to breach an asset. This could be physical local access (for example a disgruntled employee using their local account), an adjacent, connected network (e.g. a compromised LAN running between office buildings) or a public network (i.e. the Internet)
- **Potential entry and target point:** A maximum of 26 different assets could be potentially targeted and compromised and used to launch an attack
- **Length:** The maximum length into the network that an attacker could reach and the propagation length of the algorithm.

The MITIGATE algorithm was connected to a real-time port knowledge base which could quickly be updated to reflect the dynamic operation of a busy port environment.

Attack path identification was carried out using sets of rules applied to the knowledge base. Further rules also governed attack path construction.

The results of the test were positive with all possible non-cyclic attack paths quickly identified in less than two seconds.

It also enabled the further creation of a database of 182 software and hardware assets for use in more comprehensive attack path identification.

Furthermore, there was positive feedback on the user experience with the program fully web accessible, requiring no installation and including popular visualization and collaborative simulation features.

The program was also compliant with prominent security regulations and standards for the maritime sector.

CRITICAL FIRST STEP

Efficient attack path discovery is a critical part of designing a cyber defense strategy for a busy port.

This is due to the sheer number of interconnected assets and their dynamic nature.

The MITIGATE project has proven that DFS can be successfully deployed in a live port environment to quickly identify potential attack paths.

Of course, this is just the first step of the process since adequate threat mitigation measures need to be put in place to combat any incoming threats.

With continued technological evolution and collaboration, there is reason to be optimistic that the task is not an impossible one.

ABOUT THE AUTHOR

Brent Whitfield is the CEO of DCG Technical Solutions located in Los Angeles, CA since 1993. DCG provides IT Consulting for Los Angeles area businesses who need to remain competitive and productive, while being sensitive to limited IT budgets. Brent writes and blogs frequently and has been featured in Fast Company, CNBC, Network Computing, Reuters, and Yahoo Business. Because of Brent's experience as a Managed Service Provider (MSP), he is actively serving on partner advisory councils for many of the major MSP vendors providing backup, RMM, and software to the market. He also leads SMBTN – Los Angeles, a MSP peer group that focuses on continuing education for MSP's and IT professionals.

ABOUT THE ORGANIZATION

DCG Technical Solutions has been providing a generous range of network and Internet support services since 1993. Recognized for Excellence in Managed IT Services by CRN- a brand of The Channel Company, DCG was added to its 2017 & 2018 Managed Service Provider (MSP) 500 list in the Pioneer 250 category. This annual list recognizes North American solution providers with cutting-edge approaches to delivering managed services. MSP Mentor also recognized DCG among the Top 10 Fastest Growing MSPs in North America.

ENQUIRIES

Web: https://www.dcgla.com