Citi-SecureWare Software

Anonemis Research
Simenona Martinez
AnonemisResearch.com

Citi-SecureWare Software

Information Management

The IT staff establishing a computer which runs on a separate network and hard drive from the primary staff. This is a key function towards isolating attacks and allowing the IT department to also view from the perspective or "bird's eye view" of an attacker or an breach.

Software Management

IT can monitor and manage the primary network which would be authorize to monitor, record daily digital footprints, (actions, paths, file and content alterations within the system) and behaviors of the staff and most importantly, for the detection of harmful outside sources. IT department can remotely lock or power-down an employees computer who fails to meet the required muti-encryptions enforced as well as failure of updating the anti-virus software.

This software is also effective in the assessing and management of workflow and as well the effectiveness in skillset of each employee.

IT would be implementing a ***new software*** provided by a cyber-security operations management company, in this case, my own. This software would be crucial in the detection of both internal and external attacks.

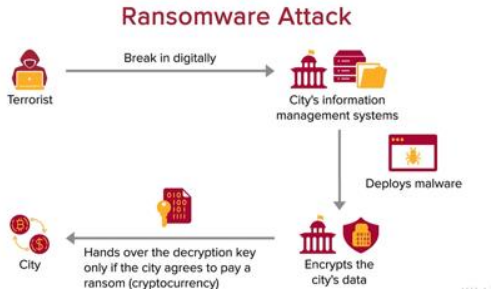
Effective in identifying the source and path of a breach, which is critical: who, what and where. For example, the approximate point of inception; the computer and agent.

Detecting where, how and when the system or files in question has changed in an operational or applicational sequence, (an abnormal sequence identical in two computers).

This would ideally and promptly, be efficient in the detecting of abnormal behaviors or data files in just one PC. This would be achieved utilizing the isolation methodology and a process, aforementioned in previous assignment, which continually tracks the sequences and behavioral data of computing at rapid pace. This detection and monitoring method would provide an instant response reaction, immediately notifying IT of the abnormalities in sequencing, trigging an automatic powering down the machine in question, isolation methodology.

This software application would also formulate a detailed analysis report upon of these immediate findings and identified pathways. This would create less footwork for an understaffed city, as well as monetary expenses.

Diagrams and report analysis would be distributed to the head of IT, a report allocating sequences found within the breach, analyzing the malware to better understand the behaviors and malware construction within the criminal enterprise. This information, depending upon city and state policy, would then be forwarded onto homeland security in an effort of compromising larger scale operations and identifying precise source locations of cyber-criminal enterprise. Most importantly, identifying the vulnerability within compromised pathway and thereby, inducing rapid correction.



Identifying allocated sequences within attacks are essential in operational and processes of recording behaviors in cyber-criminality (Cyber-Micro-Expressions). The training of software with an algorithmic system, acquiring behavioral data, thus, stopping attacks before they start by learning the patterns of the malware and it's creators.

Potentially, identifying overall patterns and sequences within the digital behavioral data pathways if information of prior attacks, offenders, and malfunctional software information is combined within agencies, acting as a gateway to finding the source of criminal enterprises, contingent upon public policy. Thus, disabling the identified primary sources, their resource data and as wells the various pathways.

Hardware Management

Mirroring Malware Signaling. This feature within the **software and hardware** would act as a two-way signal sequence once potential malware is detected. For example, rather than the infected device spreading to another, the network system hard-drive will automatically switch that device's pathway from the ***primary*** network hardware drive to an isolated network hardware-drive, separate from primary workforce.

Once this function has occurred, the potential breach or malicious file(s) which has been detected and now isolated, then begins the process of *reversed engineering malware mirror signaling*.

The encrypted filtration boxing would then act as the primary network function, meaning ***the attacker would be under the impression that they've accessed the primary hardware,***

software and/or hard drive when in fact, the malware and it's attackers has been quarantined in an isolation area.

This file would then start an immediate process of **reverse engineering** by duplicating the encryption of the malware file and signaling the very same pathway ***("Bounce")*** to send the duplicate file back to the source (***The Attacker***) with an automatic alteration of coding within the malware, ***a worm***, to collect crucial data and identify the target location.

This process all occurs while on the protected isolated network and hard-drive, while identifying the vulnerability within compromised pathway and thereby, inducing rapid correction and finally patching the pathway.

This event is concluded with a final detailed analysis report upon immediate findings, identified pathways, response reaction and lastly, the patching correction which is then sent to IT as well as other allocated departments. *Detecting, Identifying and Reporting.*

This function is also used within the description of daily apparatus, such as when downloading, emails, documents, file and spreadsheets.

This is software would efficient in doing the workload required of a larger staff, however, it offer the option of scaling it down to essential staff allocating within cities needs and budgets specific to each state, federal or city use.

.

Anonemis Research
Símenona Martínez
AnonemisResearch.com