Professional article

Tool for early detection? Or fire extinguisher in the event of damage?

When a Compromise Assessment makes sense

Compromise assessment uses forensic methods to track down attackers in the system and can thus contribute to faster detection of incidents and security incidents. But is this expensive approach also suitable for prevention? Absolutely: Because companies get an overview of whether a compromise has occurred, can determine whether security measures are effective and can take countermeasures.

Attackers are often known "ransomware groups", otherwise financially motivated groups or APTs. Ransomware enters the system because of carelessness, when links in emails containing malware or macros in Excel are clicked or activated. The attackers gather information, secure privileges and spread. Then the system is encrypted and the extortionate demand is made.

Compromise Assessment: After the attack or preventively?

As a rule, Compromise Assessment comes into play when such an attack has become known. IT experts are often faced with chaos here. Now a plan has to be set up and followed: Agents are rolled out for the scan and systems are scanned. Affected areas can be quickly identified and the investigation can thus be targeted. However, especially in large companies with many computers, it does not make sense to perform forensic analysis on every device, which would take too much time and incur enormous costs. Compromise assessment, on the other hand, identifies compromised systems, which can then be forensically examined.

According to the Mandiant Report, in 2020 an average of 76 days passed from the start of an attack to its detection[1] - this time span can be greatly reduced with Compromise Assessment.

However, Compromise Assessment is not only useful when an attacker is in the system, but also as a preventive measure. The advantages here are that the methodology allows a look into the past, which is not possible with classic IT security approaches such as EDR (Endpoint Detection and Response). Many companies do use antivirus software or

EDR; however, Compromise Assessment finds traces of attacks in the supposedly protected systems by focusing on forensic artifacts.

The problem with common cybersecurity tools: many companies weigh in believing that all you have to do is install them and they'll get the job done. But this is not so. Tools need support, they need to be adjusted and monitored, detection rules need to be adapted. Mistakes can easily be made here; with Compromise Assessment, it is possible to detect traces of cyber attacks that go beyond errors in the detection rules of the tools, for example.

Compromise assessment is possible in ad hoc use as a snapshot or continuously as Continuous Compromise Assessment. In the latter, systems are scanned at regular intervals - about once a month. Then the delta is considered: This allows traces of attackers to be found and the opportunity to react in a timely manner arises. The measures then allow for a likewise constant optimization of the security infrastructure.

Further Use Cases for Compromise Assessment

Compromise assessment is also suitable for proving during audits that enough is being done for IT security and that incidents are being documented: With such a preventive control, a statement can be made quickly as to whether there is a suspicion or active suspicious cases, an impact assessment can be made and the Incident Response Life Cycle can be triggered.

It also makes sense to use it in the case of company mergers, when networks are combined. Using an Ad Hoc Compromise Assessment of both, compromises can be identified and eliminated before opening.

Insights and information gains

Compromise Assessment also helps companies gain important insights into their cyber security; it can highlight infrastructure weaknesses: Some find that their security level is far from state of the art, and that they have been blind to the network to date. Or that assets that should be inactive were active, or that there are scripts on drives that attackers can use to gain access to admin privileges. Another possible find: service account passwords are in a file accessible to all. Policy violations can also be detected, for example when e-mails are saved as files despite instructions to the contrary, or when external devices such as USB sticks are connected without permission.

More extensive security concepts with infrastructure setup and password policies can also be started and existing measures such as anti-virus solutions and their configuration can be checked. This enables companies to eliminate vulnerabilities, reduce the likelihood of future successful attacks and raise their security level in the long term.

Benefits and limitations of Compromise Assessment

Compromise Assessment creates visibility and allows you to look into the past after installing the agent, servers and analysis. Common solutions such as EDR and SIEM do not detect problems until they are installed - and by that time, an attacker may already be on the network.

There is also a large community behind the scanner used: this has the advantage that good rules are available right from the start and the scanner is always up to date. On the other hand, it can take more time for new attack paths to be stored in an EDR, as these first have to be known to the manufacturer, who has to incorporate them and roll them out to customers. However, this time can be critical in attack detection.

Compromise assessment also has limitations. It is a passive discipline that does not invade the system automatically, and it is not a network security tool. Scans must be set up and manually triggered. Especially in the beginning, this can take time: For baselining, an inventory is first taken of all systems that are scanned and assessed. From this, measures are derived and they are checked with another scan. Evaluation also requires expertise and personnel, and thus also time - Compromise Assessment is not a discipline for quick detection. That is why it is not sufficient on its own, but is a useful addition to SIEM and EDR, for example.

As a special discipline, Compromise Assessment also requires a certain willingness to invest, because it can be expensive. Companies therefore usually start with a proof of concept on a small scale, see the potential and then roll it out across the board.

Conclusion

With Compromise Assessment, companies can constantly increase their IT security level. Attacks and their paths can be detected with a look into the past and the damage can be efficiently repaired, as the affected computers can be quickly narrowed down. But even if there

is no concrete attack, Compromise Assessment can provide a good overview of the system's vulnerabilities and countermeasures can be initiated on this basis.

[1] Mandiant (2021): *M-Trends 2021*. Online verfügbar unter: https://www.mandiant.com/sites/default/files/2021-09/rpt-mtrends-2021-4.pdf

Authors:

Christoph Lemke, Senior Cyber Defense Consultant

SECUINFRA

Leon Hormel, Cyber Defense Consultant

SECUINFRA

Further Information:

https://www.secuinfra.com/de/services/compromise-assessment/

Press contact:

SECUINFRA GmbH

Svenja Koch

Stefan-Heym-Platz 1

10367 Berlin

Mobile: +49 160 921 633 44

marketing@secuinfra.com