HOW TO DETECT & STOP SIMPLE DAY TO DAY RISKY BEHAVIORS THAT CAN LEAD TO COSTLY DAMAGING DATA LEAKS

Analysis point to the fact that 70 to 80 percent of the time, cyber-attacks come from within the corporate networks. Therefore, it is not only essential to monitor activities generating from outside the networks but as well as within.

What is the best method to detect suspicious behavior from within a corporate network? Combine data leak analysis with unusual access.

There is no point in measuring, tracking, and reporting IT security generalities when it comes to detecting abnormal situations. A far more effective approach is to focus on variations and exceptions to normal activities.

DESIGN, IMPLEMENT AND OPERATE

It is essential in terms of IT security to design architectures according to normative frameworks and best practices, to then audit, perform intrusion tests on the technological infrastructure and the applications in place. By combining these activities, it would be normal to feel in control, but the reality can be quite different. These crucial activities must be reinforced with other measures to closely observe all activity, more importantly even more so to detect what is suspicious so to be able to react rapidly rather than to be left to deal with the costly negative consequences.

As most organizations must deal with limited means in terms of money, time and resources, it is then therefore necessary to carefully choose the most important activities to be carried out from an exhaustive list.

To hope that following a design according to the regular guidelines and complete exploitation is utopian. It is impossible to do everything, to control everything and to see everything.

THE TOP 2 CRUCIAL AND ESSENTIAL ACTIVITIES

Surveillance mechanisms are very often designed to detect normal and abnormal behavior already defined. Instead, it's best to opt for a different approach that does not look for the usual trends but focuses on unusual activities & abnormalities.

STEP # 1 ANALYZE THE DATA FLOW

Data flow analysis is used to identify, control, and protect information that is backed up and in motion. The goal is to limit the leakage of sensitive data accidentally or intentionally. Data leaks are the cause of criminal acts, human errors and/or systems.

To protect against data leakage, it is required to implement a security policy, technological mechanisms and security controls.

Trends and statistics do not tell the whole story, but they reveal information that is often disturbing regarding certain network exchanges (e.g. corporate and internet emails, backup sites, exchange, and backup services, etc.), the behavior of groups of users and users. With these statistics and analyses, it becomes possible to judiciously choose samples based on a set of parameters that allow to deepen the indications and to know the reality of the network exchanges and the behaviors of the users. Certain complementary data streams (Private VPNs, Telnet, Connections, Http, Https, Databases, etc.) can also be analyzed to identify obscure exchanges of data that could lead to data leak issues. Exchange type, source, destination, amount of data, period, frequency, etc.

The solution is not in adding more technologies, but first to analyze the information already available. There is no benefit in generating more data when we do not analyze that which is already available that could reveal troubling facts.

STEP # 2 ANALYZE IDENTITIES AND UNUSUAL ACCESS

The trend is to observe and count the number of accounts, access, change requests, resolution times, etc. but generating this type of report has limited value compared to the work and costs of these activities. Of course, this information is useful and essential for exploiting environments, but it is rarely used to detect abnormal activity, risky behavior, and accounts used to leak data.

The right approach is to focus on exceptions, discrepancies, alerts, failed checks, abnormal accesses, unusual uses, suspicious, unknown, different or at-risk behaviors, an abnormal increase in data volume, abnormal uses of data, use of accounts for purposes other than their functions, etc. To be more precise, it is required to have increased monitoring to target high-privilege accounts, accounts combining multiple profiles or suddenly reused, with abnormal activities, management used for application functions, access to several non-associated files, orphan accounts used or that cross the defined boundaries.

Of course, the monitoring of these activities is not done in one single step, but it is important to start with this base and then to gradually add, specify and complete. This information will also make it possible to update the procedures, the typical use cases, the required checks, obsolete or to replace them.

WHY ARE ATTACKERS STILL FINDING GAPS IN APPLICATIONS, EXPLOITATION AND SURVEILLANCE?

They do not limit their thinking in a defined framework based on normal use. A "Thinking out of the box" approach is always constructive and offers different avenues!!! If it works for an attacker why not use this same approach to analyze what is happening? You have to build a model, cut out modules and functions to try to get around the rules.

CONCLUSION

History has clearly shown us that data leaks and abnormal application uses are not identified with conventional monitoring. Even with a well-designed and managed solution, it is critical to strengthen these activities with complementary measures to determine if data leaks occur in an environment.

Conventional approaches are always used in the exploitation of environments, but they must be complemented by innovative approaches to detect any suspicious activity. It is best to produce dashboards with a global view based on a model and supplemented by precise metrics to then direct its research, work, and analysis on elements of exceptions.

And of course, avoid adding expensive solutions and generating even more data if we do not capitalize on the information, we already have that could reveal a lot to us when we take the time to properly analyze this data.

Part # 2 Our next article will elaborate on our approach as well as our specialized dashboards that produce the essential information required to detect what is undetectable by the current efforts.

Part # 3 This article will focus on the overall management of cybersecurity. How does one get an overview of cybersecurity and track trends within a company to specific metrics?

For an INDIK™ 2.0 "Free Discovery" session, please contact us:

Alain Scherrer, Principal managing partner:
Alain.Scherrer@securecom.ca,
phone: 514 544-0442, extension 2320

Other capsules of interest on INDIK™ 2.0 will be released shortly.

+ Useful Information for IT Managers: INDIK 2.0 TI Management.pdf

https://www.indik-dashboard.com/sites/default/files/images/pdf/INDIK%202.0%20IT%20Management.pdf

+ Useful Information for Cybersecurity Managers: INDIK 2.0 Cybersecurity.pdf

https://www.indik-dashboard.com/sites/default/files/images/pdf/INDIK%202.0%20Cybersecurity.pdf

To learn more visit us at www.indik-dashboard.com

INDIK™ A Division of SecurEcom Services Conseils Inc.
368 Notre-Dame W., Suite 101
Montreal, QC
H2Y 1T9

SECURECOM indiK