CENTER FOR CYBERSIKKERHED

INVESTIGATION REPORT

NO LOGS – NO CRIME

The importance of logging as a key element in investigation of and protection against cyber threats

1st Edition October 2021

Table of contents

CENTER FOR CYBERSIKKERHED

Kastellet 30
2100 København Ø
Phone: + 45 3332 5580
Email: cfcs@cfcs.dk

1st edition October 2021.

Purpose
This investigation report outlines the importance of logging in IT systems as a key element in IT security incident analysis. Often, the CFCS is forced to discontinue its investigations due to the victims' inadequate logging. This guide is mainly intended for IT executives and IT technicians.

Summary

- Insufficient logging in IT systems is a major issue, as it hinders efforts to thoroughly investigate and counter cyber attacks.
- In 2020, the Centre for Cyber Security (CFCS) investigated an incident involving an attack against a Danish authority by a state-sponsored hacker group. This incident serves to illustrate that sufficient logging is a key element in post-incident reviews and clean-ups.
- In at least 75 per cent of the Centre's total operational cases, the investigation of cyber incidents is hampered by lack of or insufficient logging.
- The CFCS also assesses that lack of or insufficient logging hinders the efforts of numerous private security companies to fight cyber criminals.
- Logging is crucial in cyber incident investigations, although there are many other reasons why logging should be an integral part of organization practices.
- In the guide "Logging – part of resilient cyber defence", the CFCS provides recommendations for secure logging procedures.

Introduction

When the Centre for Cyber Security (CFCS) looks into potential security incidents, it asks for the logs of the affected organizations. The CFCS often encounters the problem of no logging or only insufficient logging, and in other cases where logging has in fact been enabled, the logs only cover a very short timeframe.

Insufficient logging limits the possibilities of investigating whether an organization has actually been compromised, and if so, what the hacker may have done to the organization network. Also, insufficient logging may cause uncertainty as to whether the hackers are still active in victim systems.

In a number of instances, the CFCS has been forced to completely drop its investigation into potential IT security incidents due to the lack of logging or data. Some of the incidents involved potentially serious cyber espionage attacks impacting on Danish security policy.

Good logging procedures are not only important in the sectors of society that are facing a **VERY HIGH** threat of cyber espionage. In fact, the threat posed to all parts of Danish society by cyber crime is **VERY HIGH**. As a result, Danish public authorities or private companies will highly likely fall victim to cyber attack attempts by cyber criminals. Thus, sufficient and accurate logging is a key component in the investigation and prevention of such cyber attacks. This applies to all organizations, ranging from public authorities and large corporations to small and medium-sized private companies.

This report focuses on the challenges associated with insufficient logging, based on an incident that the CFCS handled in 2020. In this concrete case, the CFCS suspected that a state-sponsored hacker group had attempted to compromise a Danish public authority. This case is a testament to the importance of sufficient logging that allowed the CFCS to investigate whether the organization was in fact attacked and analyse the hackers' tactics. The logs also made it possible to analyse whether the attack was successful.

Logging
Logs record incidents that occur in an organization network or system. Usually, log files contain a series of log lines, each describing the specific incident referred to by the log line.

Previously, logs were mainly used for troubleshooting, but today's logs can be used for multiple purposes, including network and system optimization, event tracking and not least, investigation of cyber attacks.

The CFCS has published the guide "Logging – part of resilient cyber defence". By following the recommendations outlined in the guide, organizations will be able to enjoy many of the benefits that good logging provides, including, in particular, the capability of investigating cyber attacks. Today, existing commercial systems are capable of facilitating sufficient logging in large, complex networks. However, many small-sized organizations may greatly benefit from free solutions or tools, integrated by default in, for example, Microsoft Windows.

Even though logging as such does not necessarily prevent cyber attacks, it is a key component in incident detection or investigation. One of the CFCS's missions is to examine potential cyber attacks targeting Danish public authorities or private companies that support functions vital to Danish society. However, without logs to identify the infected systems, it is very hard to provide concrete guidance.

Logs revealed that hackers monitored public authority

In the following chapters we describe a specific incident where the CFCS helped a Danish public authority investigate a cyber attack. It is highly likely that a state-sponsored hacker group was behind the attack and that the aim of the intrusion was cyber espionage. The CFCS received log files on several occasions. The extent and quality of the log files were instrumental in uncovering the entire attack.

The CFCS follows standard procedures for investigating a cyber attack, including an assessment of the extent of the incident, network vulnerabilities, possible mitigating measures, attribution and use of TTP (Tools, Tactics and Procedures) to profile a certain threat actor in order to predict and detect future similar attacks with other clients or to provide general warnings.

The CFCS employs a range of different tools and analytical methods in its work. One of the key tools is log analysis as it relatively quickly provides an insight into activities happening within victim systems. Thus, adequate and proper logging on the victim systems is fundamental to this method.

In April 2021, the CFCS contacted a Danish public authority based on a suspicion that the authority had fallen victim to an attack by a state-sponsored hacker group. The CFCS had received information that the hacker group communicated with the authority's network through specific IP addresses. Given that the public authority is connected to the sensor network, the CFCS was able to confirm that communication with the suspicious IP addresses had indeed taken place. In order to further examine the activity, the CFCS asked to review the public authority's internal log files on the assumption that the suspicious IP addresses in question would be featured in the files.

CFCS's sensor network
The CFCS regularly monitors network traffic to and from public authorities and private companies connected to the sensor network. This measure targets specifically sophisticated state-sponsored actors and other actors with access to significant financial resources.

When the CFCS received the logs from the public authority's central logging system, the CFCS could see that a threat actor had repeatedly sent queries to several of the authority's IP addresses using the suspicious IP addresses. Hackers usually tend to send this type of query to potential victims in order to map different parts of a network, using this information to pave the way for a potential compromise.

In this specific incident it was a port scanning that was used. Port scanning in itself does not necessarily raise any red flags in security systems. Normally, there are huge amounts of this type of network traffic, which is not harmful as such. Thus, the security systems are usually only able to detect malicious activity, if the IP addresses have already been identified as suspicious.

The CFCS analysts knew which IP addresses to look for and were able to see in the log files that the suspicious IP addresses had made queries to different parts of the network on different port numbers. The examples below show the closing and opening process of TCP connections.

Cyber reconnaissance
Cyber reconnaissance refers to the deliberate, often automated, technique used by malicious actors to identify, gather information and profile IT systems via the Internet looking for exploitable weaknesses. Hackers may employ different reconnaissance techniques, including vulnerability or port scanning.

Example of the first part of the log file

Apr dd 2020 tt:mm:ss: %ASA-6-302013: Built inbound TCP connection 740586367 for PUBLIC-DMZ: XXX.XXX.XXX.XXX/59819 (XXX.XXX.XXX.XXX/59819) to AUTHORITY-MAIL-DMZ: owa.authority-mail.dk/443 (owa.authority-mail.dk/443)

Log	Description
Apr dd 2020 tt:mm:ss:	Time stamp
%ASA-6-302013:	Cisco firewall with Adaptive Security Appliance (ASA)
Built inbound TCP connection 740586367	Inbound first part of a TCP 3-way handshake with event ID
for PUBLIC-DMZ:	Traffic to the network's DMZ
XXX.XXX.XXX.XXX/59819	Attacker IP-adress and port number
owa.authority-mail.dk/443	The authority's OWA mail server on port 443

Example of the second part of the log file

2020-04-dd tt:mm:ss: Local0.Info YYY.YYY.YYY.YYY 04/dd/2020:tt:mm:ss GMT: SERVERNAVN 0-PPE-1 "IPSource=XXX.XXX.XXX.XXX Host=owa2016.authority.dk URL=/owa/"

Log	Description
2020-04-dd tt:mm:ss:	Time stamp
Local0.Info YYY.YYY.YYY.YYY	Local IP-adress
SERVERNAVN 0-PPE-1	Local server-adress
"IPSource=XXX.XXX.XXX.XXX	Attacker IP-adress
Host=owa2016.authority.dk	Url-adress on the OWA-server

Figure 1: Anonymised example of the first log files sent to the CFCS.

It is possible to see from the log file example above that the hackers had made unauthorized port scans. The whole log file is written in the syslog format, but the various applications generating the log have used different formats, as indicated by the time stamps.

The first log line indicates that the public authority's Cisco firewall Adaptive Security Appliance (ASA) identifies an inbound TCP packet with the SYN flag set. Subsequently, the first step of a TCP connection is built. Thus, the log line shows that the first step of a TCP 3-way handshake process has been made. The number following "connection" is an event ID from the first step of a 3-way

handshake. Event ID allows the sorting or searching of certain incidents in the logs.

The second log line indicates that the connection shuts down again due to SYN timeout. The connection is terminated after 30 seconds awaiting 3-way handshake completion as set by the firewall. As a result, the session is not fully established.

The TCP requests displayed in the log files are a typical example of reconnaissance or a so-called active scanning using a TCP protocol. The hacker sends a query to the victim system in an attempt to test the systems' response. Depending on the type of scanning and based on the responses, the perpetrator is able to gather details about the target network, such as hardware, operating systems and open ports. At this stage, the hacker will typically store the information and use it to map the victim network and identify exploitable vulnerabilities.

Unlike the two preceding lines, a different log format is used in the third log line, which is from another application than the first two. The log line indicates that a connection is established, from an IP address to a specific server, in this case the Microsoft Office Web Application (OWA). Though the log file provides useful information in the sense that it shows that connection to the authority's OWA server was in fact established, it does not provide exact information as to the hacker's activities- only that the web server was accessed.

Thus, the different log files contained different formats. Also, the absence of cross-cutting session ID made it impossible to identify the same incident across the various applications, making it more difficult to compare logs from different systems, which is key in determining the extent of reconnaissance. Despite the various types of formats, the log files enabled the CFCS to reach a conclusion. The suspicious traffic that had prompted the investigation in the first place was highly likely network reconnaissance activity, indicating that hackers were intent on attacking the authority. However, there were no indications that the hackers had attacked yet.

Brute force attack
A (simple) brute force attack is an attack in which a hacker attempts to guess login credentials by using various combinations of letters, numbers and symbols. A software programme is able to do that very quickly. Thus, the longer a password is, the harder it is to crack. In addition to simple brute force attacks, hackers may also avail themselves of the below tactics.

Dictionary attack
Is a technique where hackers try out common words and phrases, such as those from a dictionary, to guess a password.

Password spraying
Is an attack in which the hacker attempts to access a large number of accounts with a few commonly used passwords.

Credential stuffing
Is an attack in which a hacker uses stolen usernames and passwords from one organization to access user accounts at another organization.

Missed logs showed that the authority was attacked

Following the completion of the first part of the analysis, the authority and the CFCS discovered other logs that had not been stored on the central logging system. The new logs were retrieved from a mail server, which was likely the hackers' intended target all along.

These were extensive and detailed logs relating to incidents in the specific system, once again involving a Microsoft OWA server, which is a web-based email client.

In the new logs, the CFCS was able to detect that someone had attempted to log in to a large number of email accounts. The login attempts came from the same IP addresses, which the CFCS had previously flagged as suspicious

assuming it was affiliated with a state-sponsored hacker group. The perpetrators had likely gathered a list of usernames affiliated with the authority prior to the attack. The perpetrators used the list of usernames to attempt login via the OWA server. They used a password-cracking software to try to gain access to user accounts on the system. This technique is called brute force. The figure below shows how the brute force attack was featured in the log files. The example is simplified and shows a login attempt to a single account.

Example of the new logs

Apr dd tt:mm:ss: SERVERNAME.authority.dk,
"Hostname":servernavn.myndighed.dk" "EventType":"AUDIT FAILURE",
"SeverityValue":4, "Severity":"Error", "AccountType":"User","Message":"The
Federation Service failed to validate a new credential. See XML for failure details.
<AuditResult>Failure</AuditResult> <FailureType>CredentialValidationError</
FailureType <UserId>user@authority.dk>/UserId>/
<Server>http//xx.myndighed.dk/adfs/services/trust</Server> <IpAddress>
XXX.XXX.XXX.XXX,YYY.YYY.YYY.YYY>/<IpAddress>
<ForwardedIpAddress>XXX.XXX.XXX.XXX,YYY.YYY.YYY.YYY<ForwardedIpAddress>

Log	Forklaring
Apr dd 2020 tt:mm:ss:	Time stamp
SERVERNAVN.authority.dk	The Authority's server
"EventType":"AUDIT FAILURE"	Event type - Here failed login
"SeverityValue":4, "Severity":"Error"	Value and description of error type
"AccountType":"User"	Type of user
Message":"The Federation Service failed to validate a new credential. See XML for failure details. <AuditResult>Failure</AuditResult> <FailureType>CredentialValidationError </FailureType	Description of error. Login could not be verified
<UserId>user@authority.dk>/UserId>	User
<Server>http//xx.authority.dk/adfs/ services/trust</Server> <IpAdress>	Service on the server
XXX.XXX.XXX.XXX	Attacker IP-address
YYY.YYY.YYY.YYY	Local IP-address
<ForwardedIpAddress>XXX.XXX.XXX.XXX,YYY.YYY.YYY.YYY<ForwardedIpAddress>	IP-addresses are forwarded from the load-balancer in front of the network.

Figure 2: Simplified and anonymised example of how a brute force attack could be seen in the new log file.

The box above indicates an "audit failure", caused by a login attempt from the malicious IP address XXX.XXX.XXX.XXX targeting one of the authority's IP

addresses YYY.YYY.YYY.YYY. The log also shows a ”credential validation error”, indicating that someone has made a failed login attempt to the *user[@]myndighed.dk* account. The log files do not indicate why the login failed. The login was unsuccessful either because an invalid password was entered or because the hackers were unable to bypass the two-factor authentication. The example above shows a heavily reduced log – the actual log for this specific incident comprised nearly two pages of densely written text.

Based on the log files, the CFCS analysts were able to conclude that the actor had highly likely failed to log in to any of the authority’s accounts. The authority had several security measures in place such as setting a threshold for the number of failed login attempts and the two-factor authentication system.

Consequently, based on the new logs, the CFCS was able to come to a new conclusion. Not only had the state-sponsored actor conducted reconnaissance against the authority’s systems, the actor had tried to attack the authority. Also, the attack had highly likely been blocked by the authority’s security systems.

Attack uncovered – just barely

The CFCS was only able to reach this conclusion because it had access to the necessary log files. Had there not been access to all relevant log files, the conclusion by the CFCS would have been incomplete.

In this incident the attack failed, but that is not always the case. Certainly, if the attack had been successful, the situation would obviously have been more critical. The malicious actor would have gained unauthorized access to the authority’s network and would thus have been able to move deeper into the network, making detection extremely difficult, especially without the existence of log files.

The authority had implemented security measures that subsequently led to the failure of the attack. However, it would have been easier to detect this type of attack if an extra layer of security measures had been implemented such as notifications to alert administrators about external IP addresses that attempt to log in to accounts unsuccessfully.

The analysis of the new log files also indicated that in addition to the IP addresses that the CFCS had initially labelled as suspicious, several other IP addresses had attempted to log in to numerous accounts. As a result, the analysis of the complete logs enabled the authority to detect several attempted attacks against it. As a result, the analysis prompted the authority to reconsider the possibility of revising its account lockout threshold policy.

Thus, the analysis of log files enables organizations to examine network traffic and thus, regularly adjust their security policies accordingly. However, to do so requires quality log files, and an overview of the location of the generated log files. In addition, it is vital that employees have the resources and time required to systematically analyse the log files, ultimately enabling the organization to use the logs to regularly readjust its security posture to changes in the threat landscape.

Insufficient logging – a general problem

In the specific incident mentioned, it was possible to reach a conclusion, even though the relevant log files were close to not being identified. However, in many cases identification of the correct log files is unfortunately not possible.

In at least 75 per cent of its total operational cases, the CFCS comes across the problem of insufficient logging, seriously hampering the ability to analyse IT security incidents, while at the same time making the cyber attack analysis needlessly more time consuming. As a result, valuable time is wasted – time that allows the hackers to act undisturbed inside the victim's network.

At worst, the lack of logging may force the CFCS or any other contracted security company to drop the investigation of an incident due to limited amount of data available. If hackers are operating inside the systems and sufficient analysis tools are not in place, it could have serious repercussions. Ultimately, it could prove very costly for the affected organization in case sensitive data is stolen or systems are encrypted. In some instances, it could also prove harmful to Danish competitiveness, national security and the general welfare of Danish society.

In addition to the cases that the CFCS is involved in, it also knows of other cases in which insufficient logging has created problems, including Danish companies targeted by ransomware attacks. The IT security companies contracted to bring the organization back on its feet have assessed the consequences of insufficient logging in the compromised companies as follows:

- the investigations of the attacks were needlessly time-consuming.
- the investigations were inconclusive as to how the hackers initially gained unauthorized access.
- The clean-up was extremely extensive and possibly more extensive than need be, as the investigations were unable to determine the impact of the attack.

Proper and structured logging is usually not a high priority with most organizations. Unless organizations are legally bound by regulatory logging requirements, they may be tempted to cut corners when it comes to implementing security measures that are mainly considered necessary if hit by a massive cyber attack. In this context, the CFCS often comes across:

- Inadequate logging policies and procedures.
- Insufficient log storage capacity.
- Incorrect configuration, even though proper and structured logging systems and solutions are available.
- Inadequate allocation of resources in terms of establishing, maintaining and analysing log collection capabilities
- Absence of alarm systems capable of detecting suspicious log events generated in the systems.

Below are five reasons why logging should take top priority in every organization:

Five reasons why logging should be a top priority

Adequate logging is a key element in ensuring a timely response when hit by a cyber attack. Regardless of whether internal IT employees or external security companies are tasked with investigating a security incident, their first cause of action would be to examine the logs. Consequently, the resources devoted to adequate logging will largely turn out to be a good investment.

1 Basis for investigating cyber attacks

Public authorities and private companies often fall victim to fairly sophisticated cyber attacks. Though most of the attacks are easily preventable, some of them require greater protection efforts. Thus, organizations should expect that at some point they will be faced with the need to investigate and mitigate cyber attacks. If logging is not enabled, security incident investigations would prove very difficult and, in some cases, impossible.

In some incidents, an external security company or internal IT employees may be able to examine network equipment or computers individually and ultimately reach some overall conclusions about the attack. However, the investigation may drag on, often significantly decreasing the quality.

2 Possibility to know the extent of the cyber attack

It may turn out to be a very costly affair if the extent of the compromise remains undetermined. The CFCS knows of several examples involving organizations being forced to re-establish a large share of or their whole network because the investigation failed to fully uncover the extent of the attack on the network. This has been the case in investigations that the CFCS has been directly involved in and also in cases that have been handled by private IT security companies.

Sufficient logging is fundamental to determining the extent of an attack and containing it. Instead of having to rebuild the organizational network from scratch, it will suffice to reinstall or replace the compromised software and hardware.

3 Shorter downtime in connection with cyber attack

Investigating intrusions will often be far more time-consuming if there are no system logs. Should it prove necessary to analyse server and client images instead of logs, a potential compromise will often cause an extended downtime for the individual server or client while the examination is in progress.

Downtime is a major problem and may result in revenue loss. Currently, the majority of organizations are extremely dependent on IT systems being operational at all times. Decrease in sales or production during the investigation period may leave the organization "in the red". Also, such a scenario may affect citizens and clients who rely on the public authorities and private companies and the vital services they provide. In addition, it increases the cost of the security company investigating the attack.

4 Storage is inexpensive

An increasing number of logs and more extensive logs will typically increase the need for more storage capacity. In recent years, the cost of storage has dropped dramatically and large TB (terabytes) hard drives or large amounts of cloud storage have become relatively affordable. Thus, more storage capacity is often a relatively small investment compared to many other security solutions – an investment that may prove worthwhile.

5 Overview of normal traffic pattern on network

Proper and systematic logging and subsequent analysis may contribute to developing a picture of an organization's network traffic. Once the organization knows its normal network traffic activity, it will be able to respond when something unexpected appears in the log files, either regularly in near real time or in fixed batch intervals, depending on how the systems generate and transmit logs to the central logging system.

By regularly performing log analysis and installing alarms that detect abnormal traffic patterns, it is possible to achieve some of the same effect as the so-called intrusion detection systems (IDS). IDS is the collective term for two different systems designed to monitor activity – either network-based (NIDS) or host-based (HIDS). The IDS send alerts if malicious activity is detected. If organizations have limited resources to invest in IDS, logging combined with installation of alarms for certain incidents may prove beneficial in the long run.

How to improve logging

One of CFCS's missions is to investigate potential cyber attacks against Danish public authorities and private companies that support functions vital to Danish society. However, if logging is not enabled, it becomes almost impossible to uncover the intrusion and provide situational guidance.

The CFCS has published the guide "Logging – part of resilient cyber defence", which is available on the CFCS website. The guide provides concrete recommendations on which systems logging should be a high priority. The guide also provides recommendations on which type of data should be logged on the individual systems. We recommend that the guide is read in its entirety and used as a basis to establish proper logging in organizations.

There are many commercial solutions available that may help organizations establish and organize their logging procedures, and many organizations might benefit from using some of these solutions. No matter which solutions an organization chose, it is taking steps towards strengthening its cyber security posture provided that the CFCS guidelines are followed.