CENTRE FOR CYBER SECURITY

Threat assessment

Cyber attacks against suppliers

CENTER FOR CYBERSIKKERHED

Threat assessment: Cyber attacks against suppliers

Danish Defence Intelligence Service
Kastellet 30
DK-2100 Copenhagen

Tel.: +45 33 32 55 80
E-mail: cfcs@cfcs.dk
www.cfcs.dk

Foreign states and criminals often attack their targets through the supply chain by compromising suppliers. This threat assessment is intended for companies and authorities as a tool to highlight the cyber threat facing the supply chain.

Key assessment

- Some suppliers make attractive targets for hackers as they constitute a single point of entry to multiple targets and data.
- Some hacker groups have the capabilities and intention to attack suppliers that provide key services and infrastructure to companies and authorities in Denmark.
- The Centre for Cyber Security (CFCS) assesses that this attack method is used by foreign states and cyber criminals.

Analysis

Cyber attacks against suppliers that provide key services to Danish companies and authorities constitute a cyber threat, including against sectors that are critical to the functioning of the Danish society.

Cyber attack against the supply chain is an attack method where hackers target an organization with the purpose of using it as a single point of entry to compromise its clients. In this way, hackers can access information or systems belonging to their ultimate targets.

Cyber attacks may be both politically or financially motivated.

Suppliers
In this threat assessment, suppliers are defined as any organization providing IT services, software or hardware. Suppliers may also include organizations which store client data or have access to client data. Suppliers may also outsource tasks to sub-suppliers. This threat assessment makes no distinction between suppliers and sub-suppliers.

Suppliers are attractive targets for hackers

The attack method is effective as compromising one supplier may give access to many targets, or to significant parts of a sector's infrastructure, or may make it possible to collect the supplier's customer data.

Suppliers often have unrestricted access to many of their clients' networks and data. By compromising a single supplier, an actor can potentially move unhindered between several clients' networks and data.

Actors also try to compromise suppliers across borders. There might be poorer cyber security in one branch of a supplier in a given country, which makes it easier to compromise the rest of the supplier's systems. If the supplier's networks are not segregated from its branches, it might allow the actor the possibility to move horizontally in networks across borders.

In recent years, several major international suppliers have been compromised or attempted compromised. Some of these suppliers provide services to authorities and companies in Denmark. According to open sources, the electronics giant ASUS was hacked during 2018. ASUS's official software, ASUS Live Update tool, was infected with malware. As a result, users who updated the programme downloaded a compromised version of the ASUS software, potentially giving hackers access to their computers.

Cyber attacks against Norwegian Visma

In February 2019, Norwegian software supplier Visma announced that it had been compromised. According to open sources, the purpose of the attack was to gain access to client data. Visma is a large international supplier, whose services include cloud software to companies' accounting and businesses processes. Visma also has branches in Denmark.

In recent years, a few state-backed hacker groups have turned their attention to suppliers of cloud solutions and data storage services to clients worldwide. By compromising these suppliers, the actors have secured remote access directly into client networks, enabling them to steal information. As the hackers tapped into the suppliers' secure networks, using legitimate user names and passwords, the victims found it hard to distinguish between legitimate and illegitimate activities. In some cases, the actors also gained access to client data stored on the suppliers' own servers.

Cyber attacks against cloud suppliers

According to open sources, several cloud suppliers were the targets of a comprehensive cyber attack campaign dubbed Cloud Hopper. According to open sources, the campaign targeted some of the largest international cloud suppliers, including, likely, their clients.

Other state-backed hacker groups have specifically targeted large Western legal and consultancy companies in order to gain access to relevant and often sensitive information on companies and their clients.

Accountancy firms also constitute potential targets as they host sensitive client information.
Cyber attacks have also been launched against computer manufacturers and software suppliers, infecting supplier software updates with malware that was subsequently downloaded by clients. The NotPetya attack, which hit companies such as Danish shipping company A.P. Moller-Maersk in June 2017, is one of the most well-known examples of such an attack against a software supplier.

Cyber attack against Ukrainian supplier
Ukraine-based suppliers have previously been exploited in connection with cyber attacks that have also affected Danish companies. The NotPetya attack had its origin in a compromised Ukrainian software company that developed the M.E.Doc software. Hackers compromised companies with malware through an M.E.Doc software update. The malware was a so-called worm, which quickly spread to other parts of the affected companies' IT infrastructure, infecting other companies as well.

In some cases, a supplier may no longer be able to provide security updates. Over time, the product will then come to pose an increasing security risk. A case in point is the May 2019 US Bureau of Industry and Security (BIS) list of companies, which stipulates that after a certain date US companies must obtain a special license if they wish to export to companies included on the list. Chinese company Huawei is among the entities included on the list. If effected, the ban may in the short term prevent Huawei from providing new products and security updates containing hardware components or software from US companies.

Danish organizations extensively use suppliers
Many companies and authorities in Denmark use suppliers for digital services or for services that they outsource. The services typically include cloud solutions, data storage and IT services. Many of the suppliers which are used for outsourcing are foreign and global suppliers.

From a business point of view, outsourcing can in many ways be an obvious choice as it may optimize work procedures and help companies or authorities focus their resources on core activities. Using a recognized external service provider will often have the added benefit of access to the additional security advantages provided by the major suppliers' increasingly professional measures against simple and more advanced cyber threats. Still, outsourcing may entail security challenges if the company or authority fails to formulate relevant security requirements and does not obtain sufficient insight in and control with the solution offered by the service provider. Outsourcing de facto involves leaving the protection of data and IT solutions to the supplier, even though responsibility for keeping a sufficient level of security remains with the company or authority.

Outsourcing of services to suppliers increases the threat of cyber attacks as actors may compromise many victims or key infrastructure in one fell swoop by compromising a supplier if relevant and sufficient security precautions have not been taken.

Supply chain compromises can be hard to detect
Detecting compromises or gaining insight into attempted compromise of the supply chain can be difficult as the initial targets of the compromise are not the companies or the authorities but their suppliers.

Cyber criminals attack suppliers in Business Email Compromise (BEC)

Cyber criminals have launched attacks against the supply chain by compromising supplier email accounts. Actors can leverage the compromised e-mail accounts to intercept invoices and falsify bank account details in the invoices, which are then sent on to the suppliers' clients. As the clients expect to receive an invoice for the services rendered by the supplier, the fraud can be very hard to detect.

The difficulty of detecting compromises makes it hard for companies and authorities to risk manage the supply chain threat. Once a service is outsourced to a supplier, cyber security and data access are outsourced as well. The supplier's level of cyber security, extent of preparedness, etc. automatically become subsets of the company's or authority's own measures in protecting themselves against cyber threats. Companies and authorities may find it challenging to obtain sufficient insight in, control of, and influence on such supplier procedures.

Suppliers, in turn, outsource tasks to sub-suppliers, potentially further complicating the risk management of cyber threats.

Supplier management guide
The CFCS has prepared a guide called "Information security in supplier relationships" containing a number of pointers on how to manage relations between organizations and suppliers. The guide is accessible in Danish on the CFCS website.

Threat levels
The Danish Defence Intelligence Service uses the following threat levels

NONE	No indications of a threat. No acknowledged capacity or intent to carry out attacks. Attacks/harmful activities are highly unlikely.
LOW	A potential threat exists. Limited capacity and/or intent to carry out attacks. Attacks/harmful activities are less likely.
MEDIUM	A general threat exists. Capacity and/or intent to attack and possible planning. Attacks/harmful activities are possible.
HIGH	An acknowledged threat exists. Capacity and intent to carry out attacks and planning. Attacks/harmful activities are likely.
VERY HIGH	A specific threat exists. Capacity, intent to attack, planning and possible execution. Attacks/harmful activities are highly likely.

The DDIS applies the below scale of probability