CENTRE FOR CYBER SECURITY

Threat assessment

# The cyber threat against IT service providers

**Indhold**

Threat assessment: The cyber threat against IT service providers .....1
Threat assessment: The cyber threat against IT service providers .....3
Key assessment.....3
Analysis.....3
Access makes IT service providers attractive targets for hackers .....4
IT service providers also face the threat from targeted ransomware attacks.....5
State-sponsored hackers also target IT service providers.....6
Further reading on the cyber threat against IT service providers .....7

CENTRE FOR CYBER SECURITY

Kastellet 30
2100 København Ø
Phone: + 45 3332 5580
E-mail: cfcs@cfcs.dk

1st edition November 2020

# Threat assessment: The cyber threat against IT service providers

This threat assessment is intended to inform Danish public authorities, private companies and decision-makers of the cyber threat against IT service providers, including hosting service and Managed Service Providers. Attacks against IT service providers constitute a particularly serious supply chain threat.

### Key assessment

- Cyber attacks against IT service providers pose a serious and persistent threat to Danish private companies and public authorities.
- IT service providers have legitimate, necessary and often privileged access to client IT systems and networks, making them attractive targets for hackers.
- IT service providers are both hit with targeted and opportunistic cyber attacks that are spread across many potential targets.
- Hackers carrying out cyber attacks against IT service providers are driven by different motives with criminal hackers posing a cyber threat through targeted ransomware attacks against IT service providers being one example.
- State-sponsored hackers also carry out cyber espionage against IT service providers. Such activities are both aimed at stealing intellectual property and sensitive information from public authorities.
- In addition, IT service providers have in some cases been hit by disruptive cyber attacks.

# Analysis

Cyber attacks against IT service providers not only pose a threat to the providers themselves but also to their clients.

Thus, Danish public authorities and private companies face a serious threat from cyber attacks aimed at IT service providers such as the hosting service Managed Service Providers (MSP'er), whose services they use. IT service providers typically have legitimate, necessary and often privileged access to their customers' systems. Consequently, cyber attacks against IT service providers pose a particularly serious type of supply chain threat.

# Access makes IT service providers attractive targets for hackers

IT service providers are hot targets for different types of cyber attackers, in particular cyber criminals and state-sponsored hackers. The impact of cyber attacks against IT service providers can be serious, potentially causing financial losses, operational disruptions and reputational damage.

Hackers are often drawn to IT service providers because of their access to client systems and networks. In cyber attacks against IT service providers, hackers exploit the trust and access that the service provider enjoys with its clients. Hackers will target IT service providers as entry points for compromise of their client base.

A case in point is the August 2019 infection of 22 local Texas municipalities with the REvil ransomware via an IT service provider. The hackers compromised TSM Consulting, an MSP, thereafter they used its remote access tool to deploy malware on client networks.

In another incident, in May 2020 the cloud service provider Blackbaud fell victim to a ransomware attack. Afterwards, several American and British universities have stated publicly that different types of data, for instance personally identifiable information of students and employees might be exposed as a result of the compromise at Blackbaud. The example illustrates the consequences cyber attacks against IT service providers can have for their clients.

Criminal hackers also launch cyber attacks against IT service providers with the aim of reselling the access to the service providers' IT systems and, in some cases, their client networks. This attack technique features as part of the overall threat posed by cyber crime and is not particular for attacks against IT service providers.

### IT service providers categories

**IT service providers**
For the purposes of this threat assessment, the term "IT service providers" is used collectively to describe the different types of companies below.

**Hosting service provider**
A company that runs and owns IT infrastructure offering memory- and storage capacity and computing power services to clients. A web hosting service provider is a company that provides the IT infrastructure, and technologies and services needed for a website to be viewed on the Internet.

**Managed Service Provider (MSP)**
An umbrella term for companies that offer and manage different types of IT services such as operation and support of client's in-house IT infrastructure, including back-up, patching and network monitoring services.

**Cloud service provider**
A company that runs and owns IT infrastructure across geographic locations. The client is offered remote access to dynamic and scalable server capacity, software applications like email and office-programs or a complete development platform that allows the client to develop and run their own applications and Internet services.

# IT service providers also face the threat from targeted ransomware attacks

Over the past few years, IT service providers in Denmark and abroad have fallen victim to different types of criminal cyber attacks.

In Denmark, IT service provider GlobalConnect fell victim to a ransomware attack in the autumn of 2019 and was compromised again in April 2020. The second attack also hit IT systems belonging to a number of GlobalConnect's clients, including Danish pharmaceutical procurement company Amgros.

In Denmark as well as abroad, the number of targeted ransomware attacks has risen over the past few years. In this type of attack, criminal hackers hold key IT systems hostage until a ransom fee is paid, and IT service providers are not immune to this type of attack.

**Attacks on IT service providers may affect clients' access to data**

In 2019, several foreign hosting service providers, including SmarterASP.NET whose client base counts more than 440,000 enterprises, were hit by a ransomware attack. The attack encrypted client data, leaving some clients unable to access their data for days.

Ransomware attacks against IT service providers may affect their services, and, at worst, render entire IT infrastructures inoperable for extended periods of time. Since late 2019, hackers behind targeted attacks have started leaking sensitive information stolen from victims who have refused to pay ransom. In an attack against an IT service provider, hackers could potentially gain access to sensitive information from private companies and public authorities, ultimately using this information to extort the infected IT service provider.

Collaboration exists between cyber criminals specialized in targeted attacks and cyber criminals targeting thousands of victims via phishing campaigns. Targeted ransomware attacks are often conducted following an initial opportunistic compromise of the victim network via malware distributed through phishing or via external remote access systems such as Remote Desktop Protocol (RDP) and Virtual Private Network (VPN). Sharing and sale of such initial compromises are called access-as-a-service.

# State-sponsored hackers also target IT service providers

Several states conduct cyber attacks against hosting service providers and MSPs. Much like cyber criminals, state-sponsored hackers may target IT service providers themselves or use them as entry points to specific targets among their clients. By exploiting an IT service provider's legitimate access to client IT systems and networks, hackers are able to bypass many traditional IT security precautions, such as network segmentation and control of user access rights.

**Several examples of attacks on Danish IT service providers**

In 2014-15 a Danish IT hosting company, as well as one of its clients, where compromised. CFCS assesses that the attack was carried out by state-sponsored hacker, and that the purpose of the attack was cyber espionage. The incident is described in the investigation report "KingofPhantom – bagdør til hovedmålet" (only available in Danish) available on CFCS' web site.

In 2015 a Danish IT service provider, which provides hosting to public costumers, was compromised. CFCS assesses that the purpose of the attack was to establish a network of compromised devices for further use in more cyber attacks. The attack was a part of a larger campaign described the the investigation report "Når Danmark sover – fjendtlig opmarch på usikre servere" (only available in Danish) available on CFCS' web site.

If an attack is launched using an IT service provider as a stepping stone, the specifics of the attacks may be difficult to establish. As a result, IT service providers may become attractive targets for state-sponsored hackers looking to conceal their activities.

Over the past few years, state-sponsored hackers from several countries have conducted cyber espionage campaigns against or via IT service providers, targeting companies to steal their intellectual property or public authorities to gain access to sensitive information. There are, for instance, several examples of state-sponsored hackers attacking IT service providers that provide services to governments and other authorities abroad.

Illustrative of this is the hacking of several IT and cloud solution providers as part of the "Cloudhopper" cyber espionage campaign that involved hackers accessing data from the IT service providers themselves as well as from their clients. According to several media outlets, Hewlett Packard Enterprise Co (HPE) and IBM were compromised by the hacking group known as APT10. On 20 December 2018, the US Justice Department and the FBI indicted two Chinese nationals, citing their alleged membership of APT10.

The Norwegian company Visma, that among other services deliver cloud software, was also hacked in 2019. Visma has departments in Denmark.

In addition to cyber espionage, state-sponsored hackers may also launch disruptive cyber attacks against IT service providers.

This happened in the autumn of 2019, where US and British authorities accused Russian state-sponsored hackers of launching a major disruptive cyber attack against Georgian web hosting provider Pro Service on 28 September 2019. British authorities claimed that the purpose of the attack was to generate instability and undermine Georgia's sovereignty.

The cyber attack against Pro Service resulted in the defacing of more than 2,000 Georgian websites belonging to as different victims as the Georgian government, presidential office, courts, local city councils, banks, NGOs and large businesses and news agencies. Hackers replaced the original content on the websites with a photograph of former President Mikheil Saakashvili saying "I'll be back" before shutting the websites down. However, all the websites were up and running again 24 hours later.

# Further reading on the cyber threat against IT service providers

The Centre for Cyber Security (CFCS) regularly publishes guides and threat assessments. Below is a list of publications of particular relevance to the handling of the threat against IT service providers. All publications are available on the CFCS website.

**Guide on supplier management**
"Informationssikkerhed I leverandørforhold" (only available in Danish) contains a number of recommendations on the management of relations between organizations and suppliers.

**Threat assessment on the threat against suppliers**
"Cyber attacks against suppliers" describes the general cyber threat against suppliers.

**Vejledning til anvendelse af cloudservices**
"Vejledning til anvendelsen af cloudservices" (only available in Danish) describes the principal problems that cloud services present, providing specific recommendations for assessment of the use of cloud services.

The DDIS applies the below scale of probability

| Highly unlikely | Less likely | Possible | Likely | Highly likely |
|---|---|---|---|---|

*"We assess" corresponds to "likely" unless a different probability level is indicated.*