CENTRE FOR
CYBER SECURITY

Threat Assessment

HR departments are also hit by targeted cyber attacks

Table of Contents

CENTRE FOR
CYBER SECURITY

Kastellet 30
2100 Copenhagen
Telefon: + 45 3332 5580
E-mail: cfcs@cfcs.dk

1st edition October 2020

HR departments are also hit by targeted cyber attacks

This threat assessment highlights the threat of cyber attacks against human resources (HR) professionals and systems. It is vital to protect HR departments enabling them to carry out their work without allowing hackers access to the organization. This assessment is directed mainly at authorities and companies that are critical to the functioning of the Danish society. The guidelines are directed at risk owners and technicians.

Key Assessment

- For years, hackers have launched targeted attacks against human resources (HR) departments – an attack approach that is popular with both foreign states and cyber criminals.
- Hackers attack HR departments with the purpose of using them as an entry point to compromise other parts of the private company or public authority. For instance, hackers exploit the fact that as part of their job HR professionals must often open emails and attachments from unknown sources.
- Hackers also attack HR departments as they potentially have access to valuable information and systems of interest to both foreign states and cyber criminals, including, for instance, personally identifiable information (PII) on employees.
- Hackers disguised as HR staff, exploit the reputation of the HR department to target potential job applicants.

The cyber threat against HR departments

For years, hackers have launched targeted attacks against human resources (HR) departments – a tactic that is still popular with foreign states and cyber criminals.

The cyber threat against an organization's HR department is, of course, closely linked to the overall threat facing the entire organization. The threat of cyber espionage, in particular, varies depending on which sector the organization is a part of and the type of information stored. In contrast, the threat of cyber crime is **VERY HIGH** across all sectors of society. Thus, HR departments face the same cyber threats as other organizations in Denmark, including the threat of ransomware attacks.

Hackers try to exploit HR departments as an easy entry point

Some hackers target HR departments with the goal of using them as an entry point to compromise other parts of the private company or public authority.

HR departments are generally targeted in phishing and spear phishing attacks as hackers try to exploit the fact that as part of their job HR professionals must often open emails and attachments from unknown sources.

Both foreign states aiming to conduct espionage and financially motivated cyber criminals have tried to compromise HR departments with phishing and spear phishing emails. In addition, in other countries there have been a few examples of destructive cyber attacks.

In some of these attacks, hackers send emails with fake job applications containing malware-infected links or attachments. At first glance, the attachments appear legitimate and relevant, looking like a CV, a recommendation or other documents that would normally be attached to a job application. Hackers are likely assuming that HR departments are obligated to open such emails and attachments, leading hackers to the notion that HR departments constitute an easy entry point into the systems of a private company or public authority.

Unfortunately, this assumption is supported by the fact that hackers have succeeded in compromising otherwise well-protected companies through targeted attacks against their HR departments.

Fake job application gave hackers access to central bank from which they stole USD 81 million

A well-worded but fake job application gave hackers access to Bangladesh central bank’s computers in 2015. The application appeared to be coming from a man named Rasel Ahlam, who was allegedly very excited by the idea of getting a job at the bank. An employee clicked on the attachment in the malicious email and the hackers thereby gained unauthorized access to the bank’s systems.

After being in the bank’s systems for months, the hackers managed to steal around USD 81 million from the central bank. The hackers attempted to steal close to a billion dollars, but some of the unauthorized transfers were stopped.

In 2016, fifteen million dollars were returned to the central bank of Bangladesh from a casino in the Philippines. The hackers had used the casino to launder part of the stolen money. PHOTO: Jason Arlan Raval/AP/Ritzau Scanpix

Another case in point involves the US computer and network security company RSA, which was breached by hackers in 2011, when an HR employee unwittingly opened a malicious spear phishing email. The email appeared to be coming from a legitimate recruiting company. Once the hackers gained unauthorized access, they were able to move to other parts of RSA's IT networks, stealing data involving RSA's SecurID two-factor authentication solution. RSA's customers use SecurID to protect themselves from cyber attacks. The stolen information was subsequently exploited in cyber attacks against, for instance, US defence contractor Lockheed Martin. As a result, the RSA had to replace the nearly 40 million SecurID hardware tokens used by its customers.

The RSA attack also illustrates that once hackers gain initial foothold in the HR department's systems, they may attempt to spread to other interconnected systems within the organization. Even hackers with limited technical skills are capable of carrying out such an attack. If hackers gain unauthorized access to email accounts belonging to HR professionals, they can subsequently send spear phishing emails from these accounts to other employees. Hackers exploit the fact that most employees in an organization trust that the emails sent from their HR department are legitimate.

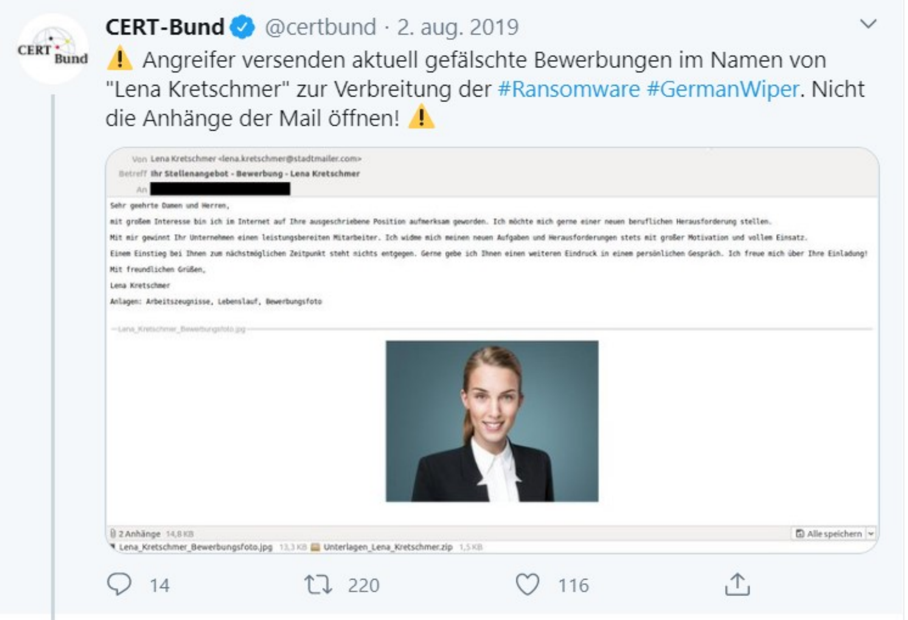
Hackers wanted to delete data by emailing fake job applications to their victims

In the summer of 2019, several organizations in Germany received an email from one Lena Kretschmer, containing a short well-written job application with an attached resume. If you opened the resume, however, you risked that malicious code would ultimately delete files on your system.

Following the file deletion process, a so-called ransom note popped up on the computer screen demanding a ransom payment in exchange for decrypting the data. However, it was actually impossible to recover the files, and CERT-EU and Europol have categorized the malware as a so-called destructive wiper malware. The malware was dubbed GermanWiper.

Few weeks later, another destructive wiper malware was delivered through fake job applications from one Eva Richter.

Both of these campaigns resembled a previous campaign in 2017 that distributed a wiper malware dubbed Ordinypt to German companies. Similarly, the malware was delivered via fake job applications.



CERT-Bund @certbund · 2. aug. 2019

⚠ Angreifer versenden aktuell gefälschte Bewerbungen im Namen von "Lena Kretschmer" zur Verbreitung der #Ransomware #GermanWiper. Nicht die Anhänge der Mail öffnen! ⚠

Von Lena Kretschmer <lena.kretschmer@stadtmailer.com>
Betreff Ihr Stellenangebot - Bewerbung - Lena Kretschmer
An [redacted]

Sehr geehrte Damen und Herren,

mit großem Interesse bin ich im Internet auf Ihre ausgeschriebene Position aufmerksam geworden. Ich möchte mich gerne einer neuen beruflichen Herausforderung stellen.

Mit mir gewinnt Ihr Unternehmen einen leistungsbereiten Mitarbeiter. Ich widme mich meinen neuen Aufgaben und Herausforderungen stets mit großer Motivation und vollem Einsatz.

Einem Einstieg bei Ihnen zum nächstmöglichen Zeitpunkt steht nichts entgegen. Gerne gebe ich Ihnen einen weiteren Eindruck in einem persönlichen Gespräch. Ich freue mich über Ihre Einladung!

Mit freundlichen Grüßen,

Lena Kretschmer

Anlagen: Arbeitszeugnisse, Lebenslauf, Bewerbungsfoto

Lena_Kretschmer_Bewerbungsfoto.jpg

2 Anhänge 14,8 KB
Lena_Kretschmer_Bewerbungsfoto.jpg 13,3 KB
Unterlagen_Lena_Kretschmer.zip 1,5 KB

The German national CERT warned about the fake job applications on Twitter. PHOTO: Cert-bund @certbund on Twitter.

Job applications are not the only theme used in phishing and spear phishing emails targeting HR departments. Another common technique among hackers is email-based impersonation attacks. This scam involves hackers sending emails that appear to be coming from a colleague or an organization that cooperates with the targeted HR department. For instance, the email impersonates an executive asking the HR professional to share employee-related information.

Hackers not only attack HR departments via fake emails, they also scan the Internet for vulnerable servers and attack vulnerable software. Both criminals and state-sponsored hackers exploit software vulnerabilities, including software used in HR departments such as HR management systems or e-learning platforms.

When hackers detect vulnerable software or servers, they may try to move on to other better protected systems. For instance, this is the case in so-called targeted ransomware attacks. In targeted ransomware attacks hackers aim to move deeper into interconnected systems in order to gain access to large or key parts of the organization’s systems. Once they have access, they encrypt the systems. It can be crippling for an organisation if key systems or data is encrypted. They then try to extort a substantial financial ransom in exchange for decrypting the data.

In Denmark, there have been several examples of targeted ransomware attacks against private companies in 2019 and 2020. Danish hearing healthcare company Demant was hit by such an attack and according to Demant’s own estimates, the attack resulted in losses running as high as DKK 650 million.

Hackers try to steal data from HR systems

In addition, hackers attack HR departments because they potentially have access to valuable information and systems of interest to both foreign governments and cyber criminals.

For example, hackers may steal sensitive data related to the organization and its employees. A case in point is the 2014 incident in which hackers compromised US authority Office of Personnel Management (OPM) that serves as the chief HR agency for the Federal Government. A committee subsequently concluded that the purpose of the attack was to steal data containing personal records on federal employees. For instance, the hackers stole information related to background checks for security clearances on 21.5 million people.

Over the past decade, both cyber criminals and state-sponsored hackers have stolen large amounts of sensitive personal information, which they may find in HR departments, among others.

65.000 employees’ personal information stolen from HR database
In 2014, a HR database at the US University of Pittsburgh Medical Center was hacked, resulting in the theft of 65,000 employees’ personal information. The data was subsequently sold on the dark web and exploited to commit extensive financial fraud.

In addition, hackers launch attacks against HR departments because HR employees have access that could be used to divert salary payments from the private company or public authority. In April 2019, hackers stole approx. USD 500,000 from a US city administration office by gaining unauthorized access to an HR application that was used to manage payroll services.

Hackers impersonate HR personnel

Hackers in attacks targeting victims outside the private company or the public authority also exploit HR departments. In these attacks, the HR employees and systems are not necessarily hacked, but rather hackers masquerade as HR personnel with the purpose of luring potential job applicants.

The hackers create fake LinkedIn profiles, send emails containing fake job offers or create fake recruitment sites. The job advertisements or websites often contain embedded malware.

The hackers try to trick the job seeker into sharing sensitive information or to gain unauthorized access to the systems installed at the job seeker's current workplace.

When a company or a public authority are exploited in this way, it can damage its overall reputation.

Recommendations

This assessment outlines a host of effective recommendations that aim to minimize the risk of hackers exploiting HR professionals to gain access to the organization.

Protect the company's employees against fake emails by validating and respecting the SPF, DKIM and DMARC email authentication policies. Similarly, the organization should implement SPF, DKIM and DMARC on their domains in order to prevent hackers from sending spoofed emails from the organization's domains. More information is available in Danish on the Danish Centre for Cyber Security's (CFCS) website.

Define and communicate requirements for the types of files that job applicants can upload or send to the HR department. Do not allow macros or other executable codes or active links. Regardless of whether the application is emailed or uploaded to a job application portal, it should be automatically scanned and analysed to detect known viruses and malware before it reaches the HR professionals. If malware is detected or the application fails to adhere to the demands outlined, it should be rejected and the sender notified.

Consider the type and amount of information shared publicly about the organization's employees and about the contact points in the organization. If applications are sent to email addresses, consider creating and using a functional mailbox and not the individual email of the HR professional. This solution will prevent unnecessary disclosure of employee-related information, which could otherwise be exploited by hackers.

Limit the possibilities of malicious code execution in the context of the employee’s user account:

- Only grant regular system user rights to HR professionals.
- Ensure that the user’s computer has an active, updated antivirus software, and that macros are disabled by default.
- Create a list of approved applications and implement application control to prevent the installation of unwanted software. This is also called application whitelisting.
- Ensure that approved programmes are continuously updated.
- Remove redundant administrator tools.

If the organization uses a job application portal, it should be tested regularly to detect potential vulnerabilities, minimum once a year and if there have been fundamental changes to the portal. The job application portal should be segregated from the other network systems, and access to it from other internal systems should be limited.

Ensure that the HR professionals are kept informed and up-to-date on the most common attack techniques, and:

- that they are aware of the cyber threat.
- that they are trained in recognizing social engineering and phishing attempts.
- that they avoid opening documents containing macros and avoid clicking on ”yes” to execute macros (given that macros are not already blocked).
- that they have the necessary awareness about sensible and safe cyber security practices, and that this knowledge is continuously maintained and updated.
- that a service desk is available in case the employee needs help with potential social engineering and phishing attacks.

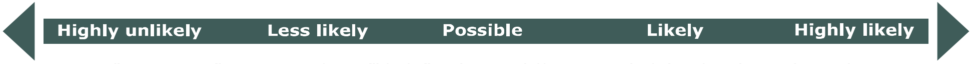
In order to prevent reputational damage, the CFCS recommends that organizations constantly keep abreast of developments on social media platforms such as LinkedIn in an effort to prevent fake profiles from exploiting the organization’s name. If fake profiles are detected, they should be reported to the social media platform in question.

Definition of threat levels

The DDIS uses the following threat levels, ranging from **NONE** to **VERY HIGH**.

NONE	No indications of a threat. No acknowledged capacity or intent to carry out attacks. Attacks/harmful activities are unlikely.
LOW	A potential threat exists. Limited capacity and/or intent to carry out attacks. Attacks/harmful activities are not 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 very likely.

The DDIS applies the below scale of probability



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