Deelbesluit 3 - Datalekken
Document 46a

12 October 2018

FINAL INCIDENT REPORT

Introduction

This report contains a brief description of the security incident in the Axiell hosting center in the Netherlands and it includes some additional details that were not in the preliminary reports that was sent out. The report also contains a description of the measures taken during the attack, measures taken directly after the attack and a description of actions that are planned in a near future.

Main conclusions presented in this report

- The attack is categorized as a "ransomware" attack.
- There are **no indications at all that any data has been leaked** from our systems.
- The **systems containing user account data was not affected by the attack.**

The security breach and measures taken

The security breach was discovered 5.1(2)h at 5.1(2)h by the System Management team through the monitoring system. Shortly after, problems were also noticed by customer service and by support.

At 5.1(2)h ransomware was discovered on several servers.

At 5.1(2)h Dutch police were contacted as well as the Dutch Cyber Collective and Fraude Helpdesk in the Netherlands.

The Axiell team has been in regular contact with CERT, the Swedish Computer Security Incident Response Team as well as with its Dutch equivalent, NCSC (the Nationaal Cyber Security Centrum). Continuous reporting was made to both agencies oral as well as written.

Our first priority was to secure customer data and our second priority to get all services up and running again. For this reason, some additional measures were taken to back up data and secure all servers before restoring. This may have caused longer downtimes, but this judgement and decision was made to make absolutely sure that no data was lost during the process.

Axiell Group AB, Box [redacted]

[redacted], tel: [redacted], e-post: [redacted]@axiell.com

The nature of the security breach

The attack was performed by someone on the outside gaining access to an administrative account through a brute force attack that permitted access to a server, using the Windows Remote Desktop Protocol.

After thorough examination of logfiles and the filesystem of the servers, we conclude that the purpose of the attack was to gain access to the servers in order to install ransomware that encrypts data. The ransomware was of the Combo/Dharma family and is well known. The ransomware was not able to automatically spread between servers and the installation on the servers had to be done manually. In addition to that, nothing else was done to the servers. Hence, our conclusion is that no data has leaked from our servers or been tempered with in any other way than the actual ransomware encryption.

The main part of the data processed by the effected systems are catalogue data for physical and digital artifacts and collections.

The data (person data) regulated by GDPR are limited to user/account data for customers that need to login and manage their systems remotely and to data captured in log-files. However, the AD itself, containing user account data, **was not** affected by the attack.

An external security expert from Fox IT was used to evaluate the security breach and advice on how to deal with it during the incident.

Actions taken during the incident

The cause of the breach was initially identified as an attack on a user account with RDP access to the servers. After the initial examination it was realized that it was an attack against our servers combined with the use of ransomware. 20 servers were affected by the security breach and the first measure taken was to shut everything down and isolate the hosting the whole hosting environment from the Internet, which also meant that all remote access to servers was shut down and additional actions were taken as listed below. This included part of the hosting environment that were not affected by the security breach, a precautionary measurement until the full scope of the breach was understood. The priorities given: securing the access to the servers, securing customer data, securing log-files and securing the servers themselves in order to protect and restore all customer setups and data.

List of actions taken

- As soon as the breach was discovered all servers where shut down.
- The servers were isolated from the Internet and al remote access was shutdown, including VPN connections to other Axiell offices.
- An "incident room" was setup onsite in the Maarssen office and all available staff was reallocated from all over Europe to the Dutch hosting center to assist.
- All log-files were secured and moved off site.
- All customer data was secured by additional backups, also of the data affected by the security breach as an extra precautionary measure.
- Customers were informed about the incident continuously (see the communication log).
- All servers where thoroughly examined, scanned and secured.
- The ransomware was removed.
- Logfiles where collected and analyzed in order to better understand the scope and purpose of the attack.
- Firewall rules where updated with the attacking IP-ranges for all Axiell hosting centers.
- All servers and all other hardware were checked for the latest security patches and working antivirus.
- All user accounts that were not absolutely necessary were disabled.
- Backups have been verified and restored.
- Password and login policies and login rules have been revised and enforced.

Communication to customers

The communication to customers was managed using the support system. The log (below) shows the communication made to customers during the security breach.

The first message to customers was sent out early on 5.1(2)h after that additional updates were sent out:

5.1(2)h [redacted]

5.1(2)h [redacted] the operations were considered normal again and all immediate aspects of the security breach had been dealt with.

Actions taken after the security breach

Some additional measures were taken, based on things learned from the incident.

- Investment in a new backup system and new routines for backups have been implemented with double backup systems on-site and off-site. The purpose is to increase redundancy and to be able to restore data significantly faster.
- The anti-virus software for the servers have been evaluated and after that it was exchanged.
- Policies for login and administrative access have been revised and will lead to future actions.

Actions planned for the future

5.1(2)h [redacted]

Contact person(s)

[redacted] (CMO) [redacted]@axiell.com, [redacted]
[redacted] (CTO), [redacted]@axiell.com, [redacted]
[redacted] (DPO), [redacted]@axiell.com, [redacted]

Deelbesluit 3 - Datalekken
Document 51a

1. PERSONAL DATA

Processor will process the following (categories of) Personal Data:

(1) Axiell collects personal data from Client contact persons. The data may concern name, gender, phone number(s), email adress, user account, job position, country and preferred language.

(2) The data collection in the application is under the responsibility of the Client. Client gets access to the application for mutating and reporting purposes.
Personal data - what can be stored in the Application:

Borrower database

Data	Description
borrower	Borrower number
name	Borrower title, forename and surname
category	Borrower category
remarks	Comments about the borrower
messages	Messages to the Borrower
bookings	Current Bookings
reservations	Current Reservations
history	What previously loaned
fines	Money owed and for what
birth	Birth date of borrower
title	Borrower title
forename	Borrower forename
surname	Borrower surname
initials	Borrower initials
Maiden name	Maiden name of the borrower (before marriage)
Sex	Gender of the borrower
ID Numbers	Any ID numbers the library would like to record
Class/department	Class or department of the borrower
Image	Photograph of the borrower
contact	Any Contacts for the borrower including address of them
Address type	Multiple addresses can be recorded explains what addresses
Address	Street
House number	House number
postcode	Postcode
City	City
Country	Country
Telephone number	Phone number
Telephone type	Multiple phone numbers can be recorded
email	Email address
Bank account number	Bank account number
Registered date	Date of registration as a borrower
Expiry date	Date of expiry of the subscription
Number of reminders	The number of overdue reminders sent
Last reminder date	The date of the last overdue reminder

Collections database

Data	Description
Acquisition from	Name of person that an object was acquired from. Links to a person record that hold details about the person.
Acquisition offer price	Price offered by the museum to the 'acquisition-from' person.
Acquisition purchase price	Price paid by the museum to the 'acquisition-from' person.
Current owner	Name of the person that owns the object. Linked to a person record that holds details about the person.
Owner history	History of owners, may be persons. Linked to a person record that holds details about the person.
From/Until	Owner of the object from/until date.
Owner's experience	Details about the owner's experience with the object.
Owner's response	Details about the owner's response (to change of ownership) regarding the object.
Acquired from	Name of (potentially) person that the owner acquired the object from. Linked to a person record that holds details about the person.
Price	Price owner paid to 'acquired-from' person.

Persons (and institutions) database

Used for the management of all kinds of person information, including staff details of the organisation using the Adlib software.

Data	Description
Name	Name (last name, first name)
Name type	Indication of context on use of the person record in other parts of the database.
Name note	Any information about the person that does not go in structured fields.
Title	Title of the person
Gender	Gender of the person
Surname	Surname of the person
Forename	First name(s) of the person
Inititals	Initials of the person
Additon(s) to the name	Any additions to the name, such as suffixes
Birth date	Date of birth
Death date	Date of death
Nationality	Nationality
Language	Language the persion speaks
Occupation	Any professional occupations of the person.
School/style	School/style of persion in the context of being an artist.
Biography	Biography of the persion.
Image	Photograph of the persion.
Address type	Multiple addresses can be recorded explains what addresses
Address	Street and house number
postcode	Postcode

City	City
Country	Country
Telephone number	Phone number
email	Email address
Fax number	Fax number
Internet address	Website related to the person
Other relationships	Any relationships with other persions or with organisations. Linked to a person/organisation record.

Deelbesluit 3 - Datalekken
Document 60a

[redacted] (Rvdr 's-Gravenhage)

Van: [redacted] (Hof Amsterdam)
Verzonden: vrijdag 21 september 2018 10:49
Aan: [redacted] (Hof Amsterdam)
Onderwerp: FW: 5.1(2)h update
Bijlagen: Personal data_collections.pdf

Onderwerp: FW: 5.1(2)h update

Geachte heer mevrouw

Zoals gecommuniceerd, heeft het hostingcentrum dat uw Axiell-applicaties beheert, een datalek waargenomen. Voor zover ons bekend, van het team dat met de crisis ter plaatse werkt, is het een lock-down van service via ransomware. We hebben de service en de firewalls gescand, maar we hebben geen sporen ontdekt die aangeven dat gegevens zijn gestolen en als we dat zouden doen, melden we dat meteen.

Er is echter de mogelijkheid dat er ongeoorloofde openbaarmaking van of toegang tot persoonlijke gegevens is geweest. We denken dat, volgens GDPR, uw gegevensverwerker, u uw gegevenssets moet beoordelen. Als u, volgens GDPR, de gegevenseigenaar vindt dat er persoonlijke gegevens in uw toepassing zijn die van toepassing zijn op de GDPR-voorschriften, moet u de GDPR-autoriteit in uw land noteren over deze datalek.
We hebben de gegevenssetinformatie toegevoegd, voor uw inzage, in de ondersteuningsaanvraag.
5.1(2)h [redacted]

Wij kunnen u voorzien van de nodige gegevens over de inbreuk op de gegevens. Onze behandeling hiervan is vanaf nu nog niet geanalyseerd en voltooid. We zullen u zo snel mogelijk informeren.
*De informatie die uw GDPR-autoriteit (**General Data Protection Regulation**) nodig heeft, kan de volgende zijn.*
• Het type inbreuk in verband met persoonsgegevens, waaronder:
a) het type en geschatte aantal getroffen personen; en
b) Het type en geschatte aantal betrokken persoonsgegevensrecords.
• De naam en contactgegevens van een contactpunt waar nadere informatie kan worden verkregen, zoals die van de functionaris voor gegevensbescherming (DPO);
• De mogelijke uitkomsten van de inbreuk in verband met persoonsgegevens; en
• Een lijst met maatregelen die zijn genomen of worden genomen om de inbreuk aan te pakken en passende maatregelen die zijn genomen om eventuele negatieve effecten te beperken.
Wij zullen, zodra we de taak hebben voltooid, u voorzien van de informatie van
• Type inbreuk
• De maatregelen die zijn genomen om deze overtreding aan te pakken en hoe toekomstige schendingen van deze aard kunnen worden voorkomen

---

Van: Servicedesk NL Mailbox [mailto:[redacted]@axiell.com]
Verzonden: woensdag 19 september 2018 16:55
Aan: [redacted]

[redacted] (Hof Amsterdam) < [redacted]@rechtspraak.nl>; [redacted] (Hof Arnhem-Leeuwarden) < [redacted]@rechtspraak.nl>; [redacted]

Onderwerp: [redacted] update

Reference: [redacted]
Summary: customer explained that sql server is unavailable since [redacted].
Supported By: [redacted]
Status: status.open

Dear Sir/Madam

As communicated the hosting center that manages your Axiell applications have experienced a data breach. To the best of our knowledge, from the team that is working with the crisis on-site, it is a lock down of service via ransomware. We have scanned the service and the firewalls, but we have not discovered any traces that indicates data has been stolen, and if we would, we will report that immediately.

There is though, the possibility of that there have been an unauthorised disclosure of or access to personal data. We think as, according to GDPR, your data processor, you should review your data sets. If you as, according to GDPR, the data owner think there is personal data in your application that apply to the GDPR regulations you have to note the GDPR authority in your country about this data breach.
We have attached the data set information, for your perusal, in the support case.

5.1(2)h [redacted]

We can supply you with the necessary data about the data breach information. Our handling of this is as of now not yet analysed and completed. We will inform you as soon as we can. The information that your GDPR authority will need may be the following.

• The type of personal data breach, including:

a) The type and estimated number of individuals affected; and

b) The type and estimated number of personal data records concerned.

• The name and contact details of a point of contact where further information can be obtained, such as that of the data protection officer (DPO);

• The possible outcomes of the personal data breach; and

• A list of measures taken or being taken to deal with the breach and appropriate measures taken to mitigate any adverse effects.

We will supply, as soon as we completed the task, you with the information of

• Type of breach

• The measures taken to handle this breach and how to avoid future breaches of this kind.

Please keep in touch with our support desk.

[redacted]
DPO Axiell Group
[redacted]@axiell.com

Deelbesluit 3 - Datalekken
Document 60aa

1. PERSONAL DATA

Processor will process the following (categories of) Personal Data:

(1) Axiell collects personal data from Client contact persons. The data may concern name, gender, phone number(s), email adress, user account, job position, country and preferred language.

(2) The data collection in the application is under the responsibility of the Client. Client gets access to the application for mutating and reporting purposes.
Personal data - what can be stored in the Application:

Borrower database

Data	Description
borrower	Borrower number
name	Borrower title, forename and surname
category	Borrower category
remarks	Comments about the borrower
messages	Messages to the Borrower
bookings	Current Bookings
reservations	Current Reservations
history	What previously loaned
fines	Money owed and for what
birth	Birth date of borrower
title	Borrower title
forename	Borrower forename
surname	Borrower surname
initials	Borrower initials
Maiden name	Maiden name of the borrower (before marriage)
Sex	Gender of the borrower
ID Numbers	Any ID numbers the library would like to record
Class/department	Class or department of the borrower
Image	Photograph of the borrower
contact	Any Contacts for the borrower including address of them
Address type	Multiple addresses can be recorded explains what addresses
Address	Street
House number	House number
postcode	Postcode
City	City
Country	Country
Telephone number	Phone number
Telephone type	Multiple phone numbers can be recorded
email	Email address
Bank account number	Bank account number
Registered date	Date of registration as a borrower
Expiry date	Date of expiry of the subscription
Number of reminders	The number of overdue reminders sent
Last reminder date	The date of the last overdue reminder

Collections database

Data	Description
Acquisition from	Name of person that an object was acquired from. Links to a person record that hold details about the person.
Acquisition offer price	Price offered by the museum to the 'acquisition-from' person.
Acquisition purchase price	Price paid by the museum to the 'acquisition-from' person.
Current owner	Name of the person that owns the object. Linked to a person record that holds details about the person.
Owner history	History of owners, may be persons. Linked to a person record that holds details about the person.
From/Until	Owner of the object from/until date.
Owner's experience	Details about the owner's experience with the object.
Owner's response	Details about the owner's response (to change of ownership) regarding the object.
Acquired from	Name of (potentially) person that the owner acquired the object from. Linked to a person record that holds details about the person.
Price	Price owner paid to 'acquired-from' person.

Persons (and institutions) database

Used for the management of all kinds of person information, including staff details of the organisation using the Adlib software.

Data	Description
Name	Name (last name, first name)
Name type	Indication of context on use of the person record in other parts of the database.
Name note	Any information about the person that does not go in structured fields.
Title	Title of the person
Gender	Gender of the person
Surname	Surname of the person
Forename	First name(s) of the person
Inititals	Initials of the person
Additon(s) to the name	Any additions to the name, such as suffixes
Birth date	Date of birth
Death date	Date of death
Nationality	Nationality
Language	Language the persion speaks
Occupation	Any professional occupations of the person.
School/style	School/style of persion in the context of being an artist.
Biography	Biography of the persion.
Image	Photograph of the persion.
Address type	Multiple addresses can be recorded explains what addresses
Address	Street and house number
postcode	Postcode

City	City
Country	Country
Telephone number	Phone number
email	Email address
Fax number	Fax number
Internet address	Website related to the person
Other relationships	Any relationships with other persions or with organisations. Linked to a person/organisation record.