Fragenkatalog „Cyberangriff / Ransomeware"

1 Telefon- und E-Mail-Erreichbarkeiten für Rückfragen

* 1. Anzeigenerstatter (Name! E-Mail / Telefon)  
     Cosfeld, Joerg. Leiter Abteilung fünf der Kunstakademie Düsseldorf.   
     joerg.cosfeld@kunstakademie-duesseldorf.de
  2. Administrator / IT-Response (Name! E-Mail / Telefon)  
     Cosfeld, Joerg. Leiter Abteilung fünf der Kunstakademie Düsseldorf.   
     [joerg.cosfeld@kunstakademie-duesseldorf.de](mailto:joerg.cosfeld@kunstakademie-duesseldorf.de)

Omieczynski, Marco. IT Mitarbeiter der Kunstakademie Düsseldorf.

[marco.omieczynski@kunstakademie-duesseldorf.de](mailto:marco.omieczynski@kunstakademie-duesseldorf.de)

1. Schadsoftware

2.1 Konnte bereits Schadsoftware festgestellt werden? Falls ja, welche?  
Es wurde keine Schadsoftware festgestellt. Die Angreifer haben sich den Standard Windows Tools bedient. Unsere AD Server wurden mittels Bitlocker verschlüsselt.

2.2 Welche Datenendung weist die Verschlüsselung auf?  
Es liegt keine Verschlüsselung in einer Datei vor. Die betroffenen Server wurden neu gestartet und damit vollständig verschlüsselt.

2.3 Ist die Verschlüsselungsart -/ Software bekannt? (Bitlocker, makop, avaddon, locky,

wannacry, Conti, andere?)  
Bitlocker

2.4 Wurde eine Textdatei (sog. Ransomenote) hinterlassen? Bitte senden Sie diese ausschließlich an folgende E-Mailadresse kk42-ck.duesseldorf polizei.nrw.de

Ein Druckauftrag mit Erpresserschreiben wurde in der Domäne der Kunstakademie an alle Netzwerkdrucker verteilt. Es wurde gedruckt bis das Papier in den Druckern leer war.

2.5 Im Falle einer Dekryptierungstestdatei: Bitte übersenden Sie diese ebenfalls an hierfür vorgesehene E-Mailpostfach kk42cceppd.nrw.de

Nicht vorhanden.

2.6 Konnte bereits festgestellt werden, auf welchem Weg die Schadsoftware auf Ihr System gelangte?

Es konnten bisher keine Vermutungen belegt werden.

2.7 Falls der Infektionsweg per E-Mail erfolgte, bitte übersenden Sie die Kopfzeilendaten / Header der E-Mail an folgendes Postfach kk42-ck.duesseldorepolizei.nrw.de

2.8 Konnte der Erstbefall welcher Datei (sog. Patient 0) festgestellt werden?

Patient 0 war der Administrator Account eines Mitarbeiters der IT-Abteilung. Anzeichen über einen brute force Angriff auf den Account sind in den Logs nicht vorzufinden.

2.9 Sind Daten im Vorfeld der Verschlüsselung abgeflossen?

Es sind laut Erpresserschreiben (siehe 2.4) Daten vom Mailserver und vom Netzwerkspeicher abgeflossen. Diese Daten umfassen Dateien aller Abteilungen und Mails aller Personen die mit der Kunstakademie aktuell in Zusammenhang gebracht werden können.

2.10 Welche Systeme (Server/Clients/Backup) sind betroffen?

Die folgenden Systeme wurden verschlüsselt:

2 x Windows Server 2019, AD#1, AD#2

Von folgenden Systemen sind Daten abgeflossen:

1x Windows Server 2019, Exchange

Darüber hinaus wurden die Daten auf folgendem Server gelöscht:

1 x Windows Server 2008R2, Netzwerkstorage

2.11 Wurden zusätzliche Admin-Konten zur Aktivierung des Verschlüsselungstrojaners durch die unbekannten Täter eingerichtet?

Ob zusätzliche Konten in der „alten“ Domain eingerichtet worden sind, ist nicht nachvollziehbar. Die Angreifer haben sich (und uns) mit dem Bitlocker aus dem System ausgesperrt. Es sind in der neuen Domain (absoluter Neuaufbau) keine fremden Admin Konten zu finden.

2.12 Konnten die verschlüsselten Daten über ein System / Backup wieder hergestellt werden?

Die beiden verschlüsselten AD-Server wurden ausgeschaltet und sind außer Betrieb. Die beiden Server konnten durch das Backup aus dem Azure AD wieder hergestellt werden.

Die Daten auf dem Netzwerklaufwerk konnten über eine Linux Distribution wieder hergestellt werden, da diese nur gelöscht, aber nicht mehrfach überschrieben wurden.

2.13 Besteht eine Online-Verbindung zum Backup oder eine physische Trennung?

Ein Backup-Server ist von dem Server, auf dem die beiden ADs virtualisiert waren, physikalisch getrennt.

3 Täterkommunikation

3.1 Im Falle einer „Lösegeldforderung". Teilen Sie bitte die Höhe der Forderung und die

Zahlungsadresse (auch digitale Währungsadressen) mit.

Es wurde kein Kontakt zu den Erpressern aufgenommen.

3.2 Welche Erreichbarkeiten wurden zur Kontaktaufnahme von den unbekannten Tätern

hinterlassen? Bitte nennen Sie diese.

jolyoga@yandex.com

3.3 Wurde bereits Kontakt von Ihnen aufgenommen? Durch Sie oder Beauftragte?

Übersenden Sie den E-Mailverkehr an das Postfach kk42ccepod.nrw.de

Es wurde kein Kontakt gesucht.

3.4 Möchten Sie Kontakt zu den unbekannten Tätern aufnehmen, ggf. auch mit Unterstützung der Polizei?

Wir möchten keinen Kontakt suchen, da der Schaden, durch unsere Arbeit, auf ein absolutes Minimum reduziert werden konnte.

3.5 Bitte teilen Sie mit, ob Sie die Forderung erfüllen oder verweigern möchten.

Verweigern

3.6 Kann Ihrerseits ein Tatverdacht geäußert werden (Ehemalige Mitarbeiter...)?

Es kann zurzeit kein Tatverdacht geäußert werden.

4 Netzwerktopologie und -konfiguration

4.1 Standort des Unternehmensservers / Backups:

Es werden mehrere Rechenzentren an mehreren Standorten betrieben. Die Virtualisierung der drei ADs und der Exchange Mailserver findet bei der Hochschule Düsseldorf statt.

Münsterstraße 156, 40476 Düsseldorf

Der Netzwerkspeicher sowie das Backup des Netzwerkspeichers befinden sich an der Kunstakademie Düsseldorf.

Eiskellerstraße 1, 40213 Düsseldorf

4.2 Art und Größe des Unternehmensservers?

Es werden nur Windows Server virutalisiert? auf HP ProLiant Gen 7 und Gen 8 betrieben.

Innerhalb der Hochschule Düsseldorf sind vier virtuelle Server auf einer Hyper V Basis zur Verfügung gestellt. Ein direkter Zugriff auf die Konsole über den Hyper V Host, ist aktuell nicht möglich.

4.3 Befindet sich der Webserver im Unternehmensnetzwerk oder bei einem Serverhoster?

Dieser befindet sich außerhalb der Netzwerklandschaft, bei einem Serverhoster.

4.4 Betriebssysteme und Versionsstände der eingesetzten Server?

siehe 2.10.

4.5 Zugangsprovider (z.B. T-Online, Vodafone, UnityMedia etc.):

Wir beziehen eine Netzspeisung über das Deutsche Forschungsnetz (DFN).

4.6 IP-Adress-Spektrum extern und intern (z.B. 195.220.198.41 — 195.220.198.50):

10.10.0.0 / 16 – Intern

193.175.67.96 - 193.175.67.127 – Extern

4.7 Netzwerktopologie (Stern, Ring, Bus, Baum):

Stern.

4.8 Anzahl der Server und Clients im betroffenen Netzwerk:

Vier betroffene Server, mit einem Client.

4.9 Name der Netzwerkdomäne und Systematik bei der Vergabe von Rechnernamen?

Die Vergabe der Rechnernamen unterliegt keiner Systematik.

Server liegen in der „kunstakademie.de“ und folgen der Systematik:

kadXXXX

4.10 Besteht ein externer administrativer Zugang zum Netzwerk (z.B. VNC, SSH etc.)?

Es bestand ein externer VPN Zugang ausgestellt über die Firewall der Hochschule Düsseldorf. Hier wird der GlobalProtect Client der PaloAlto Firewall benutzt.

4.11 Haben Kunden und / oder Mitarbeiter externen Zugriff auf das Netzwerk (z.B.

Bestellsysteme, Heimarbeitsplätze per VPN etc.)?

Mitarbeiter und Professoren haben zur Abbildung der digitalen Lehre, Zugänge auf das Netzwerklaufwerk.

4.12 Wird eine Firewall und / oder ein „Intrusion Detection System" verwandt? Falls ja,

welche(s)?

Die Kunstakademie Düsseldorf profitiert vom modernen Rechenzentrum der Hochschule Düsseldorf. Eine angemietete Standleitung (DFN) erlaubt eine direkte Netzwerkverbindung zur Hochschule. Wir befinden uns mit unseren Server in einem gesonderten VLAN und damit „hinter“ der Firewall der Hochschule Düsseldorf (PaloAlto).

4.13 Wird der Netzwerk- und E-Mail-Verkehr auf Viren überprüft? Falls ja, welche Antiviren-Software wird verwendet?

Der Mailflow wird über den DFN Spamfilter gesendet.

4.14 Wie lautet die Internet-Domain des betroffenen Unternehmens (z.B. www.firmaxvz.

de)?

kunstakademie-duesseldorf.de

5 Server- und Client-Konfiguration:

5.1 Verwendete Betriebssysteme auf den Clients?

Windows 10 oder höher.

5.2 Verwendete Dateisysteme auf Server und Clients. (z.B. NTFS, ext3, ReiserFS)?

Der Netzwerkspeicher war/ist ein Speichermedium mit NTFS.

5.3 Ist das Heim- oder Unternehmensnetzwerk lokal begrenzt oder befinden sich noch

Rechner an anderen Orten?

Oben genannte Adressen besitzen physische und virtualisierte Rechner. Mitarbeiterinnen und Mitarbeiter bekommen bei der Heimarbeit Laptops zur Verfügung gestellt.

5.4 Wer besitzt für das Netzwerk und / oder den betroffen Rechner administrative Befugnisse?

Zwei Mitarbeiter besitzen administrative Rechte für die Server.

5.5 Welche Konventionen gelten für die Vergabe von System- und Anwendungspasswörtern?

(z.B. mindestens 12-stellig mit Buchstaben, Zahlen und Sonderzeichen etc.)

Die ausgewählten Passwörter sind durch einen Generator kryptisch erstellt worden und orientieren sich am BSI Grundschutz.

5.6 Sind auf allen Netzwerkrechnern Antivirenlösungen installiert und ist eine Desktop-

Firewall aktiv? Falls ja, welche Produkte werden verwandt?

Windows Defender

5.7 Welcher Hersteller / Version der Serversoftware (MS Exchange?..) wird verwendet?

Microsoft Exchange Server 2019 (aktuellsten Updates, Stand 29.1.2022)

Name: CU11 Jan22SU

5.8 Welche Version des Domain Controllers wird genutzt?

Microsoft Windows Server Datacenter 2019 (aktuellsten Updates, Stand 29.1.2022)

5.9 Befinden sich der Server sowie der Domain Controller auf einem System?

Die Domaincontroller und der Exchange Server werden auf unterschiedlichen Maschinen virtualisiert betrieben. Sie laufen physikalisch auf dem gleichen Hostsystem, das von der Hochschule Düsseldorf bereitgestellt wird. Eine Redundanz ergibt sich aus der Ringstruktur des Rechenzentrums der Hochschule Düsseldorf.

5.10 Wird durch das Unternehmen folgende Dienste verwendet?

• Microsoft Outlook Web Access

Ja

• Active Sync

Ja

• Unified Messaging

Nein

• Exchange Control Panel (ECP) Vdir

ja

• Vergleichbarer Dienst

Nein

6 Maßnahmen zur Dokumentation und Datensicherung /

Wiederherstellung

6.1 Wann und von wem wurde der Vorfall entdeckt?

Der Vorfall wurde vom Leiter der Abteilung 5 – IT, Joerg Cosfeld am Sonntag den 30.01.2022 um 23 Uhr nachts entdeckt.

6.2 Wann, wie und von wem wurde der Vorfall untersucht und ggf. dokumentiert?

Eine IT forensische Untersuchung hat noch nicht stattgefunden. Es wurde nach der Entdeckung des Neustarts der Server über einen kompromittierten Account sofort mit dem Neuaufbau der Domain begonnen. Dieser Neuaufbau wurde von diversen Seiten aus dokumentiert.

6.3 Wurden Umbenennungen legitimer Anwendungen festgestellt (DLL Side Loading,..)

Nein.

6.4 Welche Feststellungen über den Angriff und / oder den Angreifer wurden bislang

gemacht? (z.B. Auswertung von Logfiles, Feststellung von Schadsoftware)

Logfiles des Server Management Portals wurden gesichtet um festzustellen, wann der Server für den Bitlocker, neugestartet wurde.

6.5 Existiert eine Datensicherung des betroffenen Systems vor dem Tatzeitpunkt?

Die beiden virtuellen AD Server sind abgeschaltet. Ein aktuelles Abbild der Server existiert.

6.6 Wurden im Vorfeld des Angriffs bereits Auffälligkeiten registriert? (z.B. auffällige

Port-Scans, DDoS-Attacken, Brute-Force-Attacken etc.)

Nein. Es wurden im Vorfeld keine kriminellen Aktivitäten registriert.

6.7 Befindet sich das betroffene System noch im Produktiveinsatz bzw. wann wurde es

abgeschaltet bzw. wann erfolgte u. U. die Wiederaufnahme des Betriebes?

Die betroffenen Systeme wurden abgeschaltet und sind nicht mehr in Betrieb genommen worden. Der Neuaufbau hat sofort nach der Feststellung des Sachstandes begonnen (Montag 06:00 morgens)

6.8 Wurden Logeinträge bzw. POST - Anfragen auf statische Inhalte unter dem Pfad:

/owa/auth/Current/themes/resources festgestellt, falls ja, welche?

Nein, es wurde nichts festgestellt.

6.9 Wurden Auffälligkeiten in den ECP Server Logs festgestellt (Exchange Control

Panel (ECP) Server Logs), falls ja, welche?

Nein, es wurde nichts festgestellt.

6.10 Wurden Hinweise auf sog. Webshells im System festgestellt, falls ja, welche?

Nein.

6.11 Wurden im System Hinweise auf sog. „Web Log User Agents" vorgefunden, welche

den Verdacht auf eine mögliche Kompromittierung des Systems erhärten?

Nein.

6.12 Wird eine Endpoint - Security Software im Unternehmen verwendet, falls ja, welche

Software wird wie eingesetzt?

Windows Defender

6.13 Haben Sie fachliche Unterstützung von Experten in Anspruch genommen? Falls

bitte nennen Sie uns diese mit Erreichbarkeiten.

**philipp stenzel  
senior consultant**  
itec solutions GmbH  
schirmerstrasse 76  
40211 duesseldorf  
germany  
  
fon       +49.211.417.64.30  
fax       +49.211.417.64.10

Mobil   +49.173.315.8890

mail     [Philipp.Stenzel@itec-solutions.de](mailto:Philipp.Stenzel@itec-solutions.de)

Thorsten Kunzi

glueckkanja-gab

https://www.glueckkanja-gab.com/

Thorsten Kunzi thorsten.kunzi@glueckkanja-gab.com

6.14 Wurde bereits eine IT-forensische Sicherung vorgenommen? Falls ja, durch wen?

Dipl.-Kfm.  
Manuel Rundt  
Geschäftsführer  
**IT Compliance Systeme GmbH**  
Zollstockgürtel 59  
50969 Köln  
Telefon: [+49 221 995 99 99 - 0](tel:+4922199599990)  
Telefax: +49 221 995 99 99 - 5  
Mobil: [+49 176 83 13 75 73](tel:+4917683137573)  
E-Mail: [info@compliance-systeme.de](mailto:info@compliance-systeme.de)  
Web: <https://www.compliance-systeme.de/>  
HRB 63713 Amtsgericht Köln

6.15 Wurde bereits eine Meldung an das LDI / BSI vorgenommen? Bitte übersenden Sie

diese Meldung in Kopie an kk42-ck.duesseldorfepolizei.nrw.de

7 Allgemeine Informationen / Personal / Schaden

7.1 Welche Anwendungen werden überwiegend im Netzwerk genutzt (z.B. betriebliche

Datenbanksysteme, Office-Programme, Spezialsoftware)?

Es werden alle gängigen Softwareprodukte für eine Hochschule verwendet.

7.2 Wer sind die Hauptanwender des Systems (z.B. Einkauf, Buchhaltung, Produktion)?

Mitarbeiterrinnen und Mitarbeiter, sowie das komplette Kollegium der Lehrenden.

7.3 Wer ist für die Administration bzw. Wartung des Netzwerkes, der Rechner und der

System- und Anwendungssoftware zuständig (Konkrete Nennung von Personen

oder Firmen)?

Dr. Joerg Cosfeld – Leiter der IT

Marco Omieczynski – IT Mitarbeiter

7.4 Bestehen Verdachtsmomente gegen bestimmte Gruppierungen bzw. Personen (z.B.

Mitarbeiter, Bekennerschreiben etc.)?

Nein.

7.5 Welche Angriffsszenarien gegen Ihr Unternehmen sind aus Ihrer Sicht denkbar (z.

B. Ransomware Attacke, Ausspähen wichtiger Unternehmens- bzw. Kundendaten

etc.)?

Eine „Man in the Middle“ Attacke wird vermutet.

7.6 Im Falle MS Exchange: Wurde bereits der bereitgestellte Microsoft Exchange Patch

in das betroffene System eingespielt, falls ja, wann wurde dieser Patch

durchgeführt?

Der alte Mailserver wurde auf den neusten Stand gepatched (Stand 29.2.2022).

7.7 Wurde ein externes IT - Response Unternehmen zur Detektion und Löschung

möglicher Schadsoftware beauftragt, falls ja, um welches Unternehmen handelt es

sich (Firmenname, Ansprechpartner, Anschrift, Erreichbarkeit)?

Nein.

7.8 Welcher Schaden ist Ihrem Unternehmen bislang entstanden (Bitte trennen Sie in

Kosten für bereinigende Systemadministration, Umsatzeinbußen und tatsächlichem

Schaden für mögliche inkriminierte Zahlungen an Täter, z. B. „Lösegeldforderung"

nach Verschlüsselung von Daten durch Ransomware bzw. immateriellem Schaden

durch Ausspähen von Unternehmensdaten, Reputationsverlust etc.)?

Durch unsere bisherige Arbeit ist der wirtschaftliche Schaden auf ein absolutes Minimum gehalten. Nur der Mehraufwand der IT-Abteilung ist als Schaden zu beziffern.

Kosten für die Dienstleistungen der oben benannten Personen sind hier zu nennen.

7.9 Freitextfeld / Weitere wichtige Angaben zum IT-Vorfall: