Assignment #2: Meldung an das LDI

Lecture: D3.2: Information Security and Privacy

Abgabe bis 28. Okt. 2022 - 12.00 Uhr

1. Die Dienststelle der oder des Landesbeauftragten für Datenschutz und Informationsfreiheit (LDI NRW) ist die Aufsichtsbehörde für die Verarbeitung personenbezogener Daten durch öffentliche Stellen und seit 2001 auch für nicht-öffentliche, also private, Stellen, die nicht in die Zuständigkeit des bzw. der Bundesbeauftragten für Datenschutz und Informationsfreiheit fallen.

   (a) (10p.) Erstellen Sie eine Meldung an das LDI über eine Verletzung Daten Dritter in Ihrer Institution. Ihnen ist als Verantwortlicher die Passwortliste mehrere PCs über eine Phishing Mail abhanden gekommen. **Bitte überspringen Sie die Datenfelder mit Personenbezogenen Daten.**

   Sie finden eine Vorlage der Meldung an das LDI im Anhang an diese Blatt.

Meldung einer Verletzung des Schutzes personenbezogener Daten (Art. 33 DS-GVO)

1. Art der Meldung (Art. 33 Abs. 4)

☒ Neumeldung Aktenzeichen Datum 27.10.2022

☐ Ergänzende Meldung

☒ Es stehen derzeit nicht alle Informationen zur Verfügung, eine ergänzende Meldung erfolgt voraussichtlich bis zum: 24.12.2022

~~2. Verantwortlicher (Art. 4 Nr. 7)~~

Name	
Straße	
PLZ	Ort
Telefon	
E-Mail	
Art der Stelle	
Bereich	

~~3. Meldende Person~~

Beziehung zum Verantwortlichen	
Name	
Straße	
PLZ	Ort
Telefon	
E-Mail	

~~4. Anlaufstelle für weitere Informationen (Art. 3~~3 Abs. 3 lit. b)

☐ Meldende Person

☐ Datenschutzbeauftragter

☐ Andere Person

Beziehung zum Verantwortlichen	
Name	
Straße	
PLZ	Ort
Telefon	
E-Mail	

5. Weitere an der Verletzung des Schutzes personenbezogener Daten Beteiligte

An der Verletzung des Schutzes personenbezogener Daten sind Dritte (z.B. Auftragsverarbeiter (Art. 4 Nr. 8), gemeinsam Verantwortlicher (Art. 26 Abs. 1)) beteiligt. ☒ ja ☐ nein

6. Bekanntwerden der Verletzung des Schutzes personenbezogener Daten

Zeitpunkt/-raum der Verletzung des Schutzes personenbezogener Daten:

☒ am 27.10.2022

☒ von ganztäglich bis

Zeitpunkt des Bekanntwerdens der Verletzung des Schutzes personenbezogener Daten:

Begründung der Verzögerung, falls Meldung nicht binnen 72 Stunden erfolgt (Art. 33 Abs. 1)

entfällt.

Wie wurde die Verletzung des Schutzes personenbezogener Daten bekannt?

Am Samstag, dem 29.01.2022 ab 15.00 Uhr, funktionierte nicht mehr die Telefonanlage und das Versenden von E-Mails war nicht mehr möglich. Beim Überprüfen der Anlagen wurde festgestellt, dass die beiden Active Directory Server gesperrt sind. Am Sonntagabend besichtigte die IT die Anlagen vor Ort und es fiel auf, dass die Drucker unzählige Schreiben gedruckt hatten, bis das Papier aufgebraucht war. Am Sonntag, dem 20.01.2022 gegen 23.00 Uhr fiel auf., dass ein weiterer Server (Storage Server) verschlüsselt ist und eine Modifikation an einem Shibboleth-Server vorlag.

7. Beschreibung der Verletzung des Schutzes personenbezogener Daten

Art der Verletzung des Schutzes personenbezogener Daten (Art. 33 Abs. 3 lit. a, Art. 4 Nr. 12)

- ☐ Vernichtung
- ☒ Verlust
- ☒ Veränderung
- ☐ Unbefugte Offenlegung
- ☐ Unbefugter Zugang

Erläuterung:

Aufgrund des unberechtigten Zugangs (keine willentliche Weitergabe der Kunstakademie an die Angreifer erfolgt) auf die Admin User konnten wichtige Server der Hochschule gesperrt werden. Insbesondere wurden nach derzeitigem Erkenntnisstand die beiden Active Directory Server und der Storage Server gesperrt, bzw. verschlüsselt. Zudem wurden über den Zugriff auf das Netzwerk der Hochschule die Drucker bedient und ein Schreiben mit erpresserischem Inhalt wurden vielfach ausgedruckt.

Wie kam es zu der Verletzung des Schutzes personenbezogener Daten?

- ☐ Weitergabe von personenbezogenen Daten an Unbefugte
- ☐ Fehlversand
- ☐ Veröffentlichung
- ☐ Offener E-Mailverteiler
- ☐ Diebstahl eines Mediums mit personenbezogenen Daten
- ☒ Verlust eines Mediums mit personenbezogenen Daten
- ☐ Zerstörung eines Mediums mit personenbezogenen Daten
- ☒ Hackerangriff (Virus/Trojaner/Phishing)

Erläuterung:

Eine Weitergabe von personenbezogenen Daten an Unbefugte kann derzeit weder bejaht noch ausgeschlossen werden. Es wurden über die All-in-One Drucker der Hochschule Schreiben ausgedruckt, in denen für das Entsperren der Server um Kontaktaufnahme unter Angabe einer Adresse (jolyoga(….@yandex.com) zur Zahlung eines Lösegelds gebeten wurde. So wird erstmal vermutet, dass eine Weitergabe der Daten bis zu diesem Zeitpunkt noch nicht erfolgt ist. Die Vermutung ist, dass ein Shibboleth- Server modifiziert wurde und bei der Einbindung von eBooks für die Bibliothek so die Zugangsdaten der Admin User an jemand Unberechtigtes weitergeleitet wurden.

Wer oder was hat die Verletzung des Schutzes personenbezogener Daten ausgelöst?

- [ ] Technischer Fehler
- [x] Person mit Schädigungsabsicht
- [ ] Person ohne Schädigungsabsicht
- [ ] unbekannt

8. Beschreibung der betroffenen Personen und Daten

Kategorien betroffener Personen (Art. 33 Abs. 3 lit. a)

- [ ] Kinder/Minderjährige
- [ ] Kunden oder Kundinnen
- [x] Beschäftigte
- [ ] Nutzer oder Nutzerinnen
- [ ] Patienten oder Patientinnen
- [ ] schutzbedürftige Personen

Lehrende, Verwaltungsmitarbeiter und Studierende

Kategorien betroffener Daten (Art. 33 Abs. 3 lit. a)

Besondere Kategorien personenbezogener Daten (Art. 9 Abs. 1)

- [ ] Daten zur rassischen und ethnischen Herkunft
- [ ] politische Meinungen
- [x] religiöse oder weltanschauliche Überzeugungen
- [ ] Gewerkschaftszugehörigkeit
- [ ] genetische Daten
- [ ] biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person
- [ ] Gesundheitsdaten
- [ ] Daten zum Sexualleben oder zur sexuellen Orientierung

Sonstige Kategorien

- [x] Finanzdaten
- [ ] Daten aus dem Versicherungsbereich
- [x] E-Mail-Adressen
- [ ] Passwörter
- [x] Geheimhaltungs- oder Verschwiegenheitspflichten unterliegende Daten
- [x] Postadressen
- [ ] Standortdaten
- [ ] Fotos/Videos

Ungefähre Zahl betroffener Personen (Art. 33 Abs. 3 lit. a) 650 Personen

Ungefähre Zahl betroffener Datensätze (Art. 33 Abs. 3 lit. a)

Ergänzende Bemerkungen: Kategorien Daten der Studierendenverwaltung, der Finanzverwaltung und der Personalabteilung der letzten 1,5 Jahre auf dem von den Angreifern gesperrten Storage-Server

9. Folgen der Verletzung des Schutzes personenbezogener Daten

Welche Folgen hat die Verletzung des Schutzes personenbezogener Daten wahrscheinlich für die betroffenen Personen (Art. 33 Abs. 3 lit. c) ?

- [ ] Identitätsdiebstahl
- [x] Betrug
- [ ] finanzielle Verluste
- [ ] Gefährdung des Berufsgeheimnisses
- [x] Verlust der Kontrolle ihrer personenbezogener Daten
- [ ] Einschränkung von Rechten
- [ ] Diskriminierung
- [ ] Aufhebung der Pseudonymisierung
- [x] Rufschädigung
- [x] erhebliche wirtschaftliche Nachteile
- [ ] erhebliche gesellschaftliche Nachteile
- [ ] Gefahr für Leib und Leben

Erläuterung:

Welches Risiko für die Rechte und Freiheiten betroffener Personen besteht nach aktuellem Kenntnisstand voraussichtlich (Art. 33 Abs. 3 lit. c)?

- [ ] voraussichtlich kein bzw. nur geringes Risiko
- [x] Risiko
- [ ] hohes Risiko

Begründung:

10. Maßnahmen zur Behebung oder Abmilderung der Verletzung des Schutzes personenbezogener Daten

Wurde die Verletzung des Schutzes personenbezogener Daten beseitigt? [x] ja [ ] nein

Begründung:

Welche Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten hat der Verantwortliche ergriffen bzw. schlägt er vor (Art. 33 Abs. 3 lit. d)?	Der Shibboleth- Server wurde direkt abgeschaltet, der E-Mail- Server und der Server der Telefonanlage wurden vom Netz genommen. Die Domain wurde gewechselt und die Druckserver neu aufgesetzt. Der stellvertretende CISO der Kunst- und Musikhochschulen wurde mit eingebunden. Der Server der Telefonanlage und der E-Mailserver wurden neu aufgesetzt. Außerdem wurden die beiden Active Directory Server, in der neuen Domäne, komplett neu aufgesetzt.
Welche Maßnahmen zur Abmilderung möglicher nachteiliger Auswirkungen hat der Verantwortliche ergriffen bzw. schlägt er vor (Art. 33 Abs. 3 lit. d)?	Anzeige bei der Polizei erstatten und hier weitere Schritte zur Kontaktaufnahme mit den Angreifern besprechen; mit Hilfe eines Dienstleisters eine Entschlüsselung der Server erreichen

11. Benachrichtigung der betroffenen Personen (Art. 34)

☒ Die betroffenen Personen wurden nicht benachrichtigt, da voraussichtlich kein hohes Risiko für die Rechte und Freiheiten betroffener Personen besteht.

Die betroffenen Personen wurden benachrichtigt (Art. 34 Abs. 1)

☐ Es handelt sich um eine Verarbeitung personenbezogener Daten, die im Rahmen der Tätigkeiten von Niederlassungen eines Verantwortlichen oder eines Auftragsverarbeiter in mehr als einem Mitgliedstaat nach Art. 4 Nr. 23 lit. a erfolgt.

Es handelt sich um eine Verarbeitung personenbezogener Daten die erhebliche Auswirkungen auf betroffene Personen aus dem Bereich weiterer EU-Staaten / Europäischer Wirtschaftsraum (EWR) Mitgliedsstaaten nach Art. 4 Abs. 23 lit. b hat oder haben kann.