Bundesamt
für Sicherheit in der
Informationstechnik

Meldeformular gemäß § 8b Absatz 4 BSIG

0. Allgemeine Informationen zum Meldenden

0.1	Name oder ID des meldenden Unternehmens bzw. der meldenden GÜAS	Trinkwasser-Mustergewinnungswerk
0.2	Betroffene Anlage (Name)	Trinkwasser-Mustergewinnungswerk
	Betroffene Anlage (Ort)	Musterstadt
0.3	Name des Ansprechpartners für technische Rückfragen	Frau Erika Mustermann
0.4	Kontaktdaten des Ansprechpartners (E-Mail)	e.mustermann@twgw.muster
	Kontaktdaten des Ansprechpartners (Telefonnummer)	0000 - 99 99-9099

☐ Die nachfolgenden Informationen sind bereits erfasst unter der folgenden Registrierungsnummer
(Felder 0.5 bis 0.10 müssen in diesem Fall nicht ausgefüllt werden)

0.5	Name des Hauptansprechpartners	Herr Max Mustermann
0.6	E-Mail	it-sig@twgw.muster
0.7	Telefon (Festnetz)	0000 - 99 99-9090
0.8	Telefon (Mobil)	0000 - 99 99-999
0.9	Fax	0000 - 99 99-9091
0.10	Notfallkommunikationssysteme (z. B. Satellitentelefon)	

1. Allgemeine Informationen zum Vorfall

1.1 Meldungsart

- ☐ Freiwillige Mitteilung ohne gesetzliche Verpflichtung
- ☒ Erstmeldung gemäß gesetzlicher Verpflichtung gem. § 8b Absatz 4 BSIG
- ☐ Folgemeldung zu Meldungsnummer
- ☐ Abschlussmeldung zu Meldungsnummer

1.2 Wie ist Ihre aktuelle Lageeinschätzung?

☐	Rot	Ausfall der kritischen Versorgungsdienstleistung auf lokaler, regionaler, nationaler Ebene erwartet bzw. eingetreten
☒	Orange	Beeinträchtigung der kritischen Versorgungsdienstleistung bis hin zum Notbetrieb erwartet bzw. eingetreten
☐	Gelb	Verstärkte Auffälligkeiten in der Kritischen Informationsinfrastruktur, aber keine Beeinträchtigung der Versorgungsdienstleistung eingetreten, oder es werden nur geringe Beeinträchtigungen erwartet
☐	Grau	Keine Auffälligkeiten in der Kritischen Informationsinfrastruktur

1.3 Zeitpunkt des letzten in die Meldung eingeflossenen Sachstands

Datum: 01.04.2016 Uhrzeit: 13:37

1.4 Betroffener Sektor / betroffene Branche

Energie
- ☐ Elektrizität
- ☐ Gas
- ☐ Mineralöl
- ☐ Fernwärme

Finanz- und Versicherungswesen
- ☐ Banken
- ☐ Börsen
- ☐ Versicherungen
- ☐ Finanzdienstleister

Transport und Verkehr
- ☐ Luftfahrt
- ☐ Binnenschifffahrt
- ☐ Seeschifffahrt
- ☐ Schienenverkehr
- ☐ ÖPNV
- ☐ Straßenverkehr
- ☐ Logistik

Informationstechnik und Telekommunikation
- ☐ Telekommunikation
- ☐ Informationstechnik

Wasser
- ☒ Öffentliche Wasserversorgung
- ☐ Öffentliche Abwasserbeseitigung

Gesundheit
- ☐ Medizinische Versorgung
- ☐ Arzneimittel und Impfstoffe
- ☐ Labore

Ernährung
- ☐ Ernährungswirtschaft
- ☐ Lebensmittelhandel

1.5 Welche kritischen Dienstleistungen gem. BSI-KritisV sind betroffen?

Trinkwasserversorgung

1.6 Welche Anlagentypen gem. BSI-KritisV sind betroffen bzw. könnten betroffen sein?

Gewinnungsanlage

2. Beschreibung der IT-Störung

2.1 Welche Grundwerte der Informationssicherheit wurden verletzt?

- ☒ Verfügbarkeit
- ☒ Integrität
- ☐ Authentizität
- ☐ Vertraulichkeit

2.2 Auf welchem/r IT-System / IT-Prozess / IT-Komponente ist was aufgetreten?

Fehlfunktion und Abstürze der PC-gestützten Pumpensteuerung

2.3 Wie ist es aufgetreten?

Konfigurationsdateien des Programms zur Pumpsteuerung wurden mit Locky verschlüsselt

2.4 Welche (erfolgreichen) Gegenmaßnahmen wurden eingeleitet?

Locky wurde vom PC entfernt, Neuinstallation beauftragt

2.5 Datum und Uhrzeit, an dem die IT-Störung eingetreten ist

Datum: 31.03.2020 Uhrzeit: 20:00

2.6 Datum und Uhrzeit, an dem die IT-Störung entdeckt wurde

Datum: 01.04.2020 Uhrzeit: 08:00

2.7 Die IT-Störung hält noch an

- [x] Ja
- [ ] Nein - Dauer (dd:hh:mm):

2.8 Wie ist die IT-Störung aufgefallen?

- [x] Systemausfall
- [ ] Systemwartung
- [ ] Hinweise von Dritten
- [ ] Hinweise des BSI
- [x] Fehlverhalten von Systemen
- [ ] Technisches (Netz-)Monitoring
- [ ] Veröffentlichung von gestohlenen Informationen durch Dritte
- [ ] Auswertung von Logfiles
- [ ] Testbetrieb
- [ ] Audit, Prüfung, Zertifizierung
- [ ] Sonstiges:

3. Vermutete oder tatsächliche Ursachen (Mehrfachnennungen möglich)

3.1 Physikalische Schäden

- [ ] Zerstörung von Geräten
- [ ] Diebstahl von Geräten
- [ ] Manipulation von Geräten
- [ ] Verlust von Geräten
- [ ] Sonstiges:

3.2 Technisches Versagen

- [ ] Versagen von Hardware
- [ ] Überlastung
- [ ] Software fehlerhaft
- [ ] Fehlverhalten von Systemen
- [ ] Sonstiges:

3.3 Organisatorische Ursachen

- [ ] Fehlbedienung
- [ ] Unautorisierte Nutzung von Ressourcen
- [ ] Social Engineering
- [ ] Sonstiges:

3.4 Versagen der genutzten Infrastruktur

- ☐ Stromausfall
- ☐ Netzwerkausfall
- ☐ Kühlungsausfall
- ☐ Sonstiges:

3.5 Technischer Angriff

Ausnutzung von Schwachstellen

- ☐ Nutzung von Systemressourcen (Spam-Relay, Botnetz-Client, C&C-Server, Dropzone-Server)
- ☐ Code Execution
- ☐ Protokollschwachstelle
- ☐ Privilege Escalation
- ☐ Injection-Angriff
- ☐ Cross-Site-Scripting
- ☐ Cross-Site-Request-Forgery
- ☐ Schwache Algorithmen/Schlüssel
- ☐ Sonstiges:

Missbrauch (Innentäter)

- ☐ Weitergabe interner Informationen
- ☐ Unberechtigtes Erlangen von besonderen Zugriffsrechten, z. B. von Administrations-rechten
- ☐ Missbräuchliche Nutzung von Berechti-gungen (insb. von Zugriffsrechten), z. B. durch Externe
- ☐ über Fernwartungszugänge
- ☐ Sonstiges:

Gezielte, mehrstufige kombinierte Angriffe (APT-Angriffe)

- ☒ Initialer Angriff per E-Mail
- ☒ Initialer Angriff über Webseiten (Watering hole attack)
- ☒ Initialer Angriff über manipulierte Hardware (z. B. USB-Stick)
- ☐ Sonstiges:

Hacking und Manipulationen

- ☐ Webanwendungsbasierte Angriffe, z. B. Drive-by-Exploits
- ☐ Angriffe auf Webanwendungen, z. B. SQL-Injection, Buffer Overflow
- ☐ Angriffe auf Anwendungen bzw. Dienste wie DNS, SMTP, FTP
- ☐ Systematisches Ausprobieren von Passwörtern
- ☐ Sonstiges:

Schadprogramme (Malware)

- ☒ Malware-Infektion, z. B. durch Trojaner, Rootkits zum Zwecke der Kontrollübernahme, der Datenmanipulation oder des Datenabflusses
- ☒ Ransomware z. B. Sperren von IT-Systemen zu Erpressungszwecken
- ☐ Adware, Scareware z. B. zu Betrugszwecken
- ☐ Multifunktionale Malware z. B. Viren, Würmer, Riskware
- ☐ Sonstiges:

Identitätsmissbrauch

- ☐ Verschleierung einer Identität
- ☐ Diebstahl von Zugangsdaten, z. B. Identitätsdiebstahl, Phishing, Spear-Phishing, Pharming, Skimming
- ☐ Diebstahl oder Fälschung von Zertifikaten
- ☐ Unrechtmäßige Registrierung von Internetdomänen (Cybersquatting)
- ☐ Sonstiges:

Verhinderung von Diensten

- ☐ Überflutung, z. B. (D)DoS
- ☐ Gezielter Systemabsturz, z.B. Paketfragmentierung
- ☐ Sonstiges:

Sonstiges

- ☐ Sonstiges:

3.6 Sonstiges (z. B. CVE, Name der Schadsoftware, weitere Informationen) Locky

4. Allgemeine Informationen zum informationstechnischen Angriff

☐ Es handelt sich **nicht** um einen informationstechnischen Angriff

4.1 Technischer Angriff

- ☐ Gezielter Angriff
- ☐ Ungerichteter Angriff
- ☒ Unbekannt

4.2 Bei mehrfachen Angriffen bitte vermutete Anzahl angeben

4.3 Vermutete Motivation (freiwillige Aufgabe, Mehrfachnennungen möglich)

- ☒ Unbekannt
- ☒ Finanziell
- ☐ Persönlich
- ☐ Politisch
- ☒ Kriminell
- ☐ Terroristischer Hintergrund (Pflicht für das BSI zur Weitergabe der Meldung an BKA)
- ☐ Nachrichtendienstlicher Hintergrund (Pflicht für das BSI zur Weitergabe der Meldung an BfV)
- ☐ Sonstiges:

4.4 Welche Daten sind im Rahmen der bisherigen Analyse der IT-Störung angefallen und können dem BSI zur Verfügung gestellt werden?

- ☐ Malware Samples
- ☐ Hashsummen
- ☐ Dateinamen
- ☐ Signaturen
- ☐ Logfiles
- ☐ IP-Adressen
- ☐ URLs
- ☒ Sonstiges:

Keine / unbekannt / Administratoren untersuchen noch

4.5 Strafverfolgung

Wenn eine Strafanzeige gestellt wurde und Sie eine Weiterleitung an das BKA wünschen, ergänzen Sie bitte die entsprechenden Detailangaben.

- [x] Unbekannt / keine Angabe
- [ ] Es wurde keine Strafanzeige erstattet
- [ ] Strafanzeige wurde gestellt

Aktenzeichen:

Polizeidienststelle:

Bundesland:

- [ ] Weiterleitung der Meldung an BKA durch BSI ist erwünscht
- [ ] Täter wurde ermittelt

5. Informationen zum Ausfall bzw. zur Beeinträchtigung der kritischen Dienstleistungen

5.1 Hat die IT-Störung zu einem Ausfall oder zu einer Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur (also der kritischen Dienstleistungen) geführt?

- [ ] Ja, zu einem Ausfall
- [x] Ja, zu einer Beeinträchtigung
- [ ] Nein (dann kein Ausfüllen der Felder 5.6 bis 5.8 notwendig)

Wenn nein: Welche Umstände oder Gegenmaßnahmen führen dazu, dass es nicht zu einer Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur kommt?
(Bsp.: Unabhängige Parallelversorgung, Angreifer wurde vorher aufgehalten, etc.)

5.2 Inwiefern ist die Funktionsfähigkeit der Kritischen Infrastruktur (also die Verfügbarkeit der kritischen Dienstleistungen) beeinträchtigt bzw. **könnte** sie beeinträchtigt werden?
(u. a. welche Systeme und Komponenten sind betroffen bzw. könnten betroffen sein?)

Die Wasserpumpe "Mustermündung" arbeitet unregelmäßig und liefert nur noch einen Bruchteil der im Normalbetrieb gewonnenen Wassermenge.

5.3 Wie viele Personen könnten nach Ihrem Kenntnisstand von der Beeinträchtigung / dem Ausfall der Funktionsfähigkeit der Kritischen Infrastruktur betroffen sein?

- [ ] < 250.000 Einwohner (bzw. < 50 % der in der BSI-KritisV für Ihre Anlage angegebenen Schwelle)
- [x] 250.000 bis 500.000 Einwohner (bzw. 50 % bis 100 %)
- [ ] 500.000 bis 1.000.000 Einwohner (bzw. 100 % bis 200 %)
- [ ] 1.000.000 bis 5.000.000 Einwohner (bzw. 200 % bis 1000 %)
- [ ] > 5.000.000 Einwohner (bzw. > 1000 %)
- [ ] Es kann keine Aussage gemacht werden

5.4 Wie ist die (potenzielle) geografische Verbreitung der Beeinträchtigung / des Ausfalls der Funktionsfähigkeit der Kritischen Infrastruktur (also der kritischen Dienstleistungen)? (Stadt, Region, Landkreis, Bundesland, Bundesgebiet)

Musterstadt und umliegender Kreis

5.5 Ist der Vorfall (potenziell) grenzüberschreitend?

☐ Ja
☒ Nein

Wenn ja: Welche Staaten sind / wären ebenfalls betroffen?

5.6 Von wann bis wann bestand die Beeinträchtigung / der Ausfall der Funktionsfähigkeit der Kritischen Infrastruktur (also der kritischen Dienstleistungen)?

Von ca. Datum: Uhrzeit:

Bis ca. Datum: Uhrzeit:

☒ Auswirkung dauert an

5.7 Wann wurde die Beeinträchtigung / der Ausfall der Funktionsfähigkeit der Kritischen Infrastruktur (also der kritischen Dienstleistungen) festgestellt?

Am ca. Datum: 01.04.2016 Uhrzeit: 08:00

5.8 Welche Maßnahmen wurden ergriffen, um die Beeinträchtigung / den Ausfall der Funktionsfähigkeit der Kritischen Infrastruktur (also der kritischen Dienstleistung) zu mindern oder zu beheben?

Suche nach Original-Konfigurationsdateien

6. Sonstiges

6.1 Weiterführende Informationen

6.2 Weiterführende Bewertungen

6.3 Weiteres