Meldeformular

nach § 8b Absatz 4 BSIG

0. Allgemeine Informationen zum Meldenden

0.1	Name des meldenden Unternehmens bzw. der meldenden GÜAS	Trinkwasser-Mustergewinnungswerk
0.2	Betroffene Anlage (Kritische Infrastruktur gemäß BSI-KritisV) (Name und Ort)	Trinkwasser-Mustergewinnungswerk, Musterstadt
0.3	Name des Ansprechpartners für technischen Rückfragen	Frau Erika Mustermann
0.4	Kontaktdaten des Ansprechpartners (E-Mail, Telefonnummer)	e.mustermann@twgw.muster, Tel.: 0000 – 99 99-9099
	Die nachfolgenden Informationen sind bereits erfasst unter der Registrierungsnr.: (dann kein Ausfüllen der Felder 0.5-0.10 notwendig)	
0.5	Name des Hauptansprechpartners (Kontaktstelle gemäß § 8b (3) BSIG)	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 (Mehrfachnennungen möglich)	☐ Freiwillige Mitteilung ohne gesetzliche Verpflichtung ☒ Erstmeldung gemäß gesetzlicher Verpflichtung BSIG §8b (4) ☐ Folgemeldung zu IT-Störungsnummer: ☐ Abschlussmeldung zu IT-Störungsnummer:
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, Uhrzeit)	01.04.2016, 13:37 Uhr
1.4	Betroffener Sektor bzw. betroffene Branche	

Energie
- ☐ Elektrizität
- ☐ Gas
- ☐ Mineralöl

Ernährung
- ☐ Ernährungswirtschaft
- ☐ Lebensmittelhandel

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

Wasser
- ☒ Öffentliche Wasserversorgung
- ☐ Öffentliche Abwasserbeseitigung

Informationstechnik und Telekommunikation
- ☐ Informationstechnik
- ☐ Telekommunikation

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

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

1.5	Welche kritischen Dienstleistungen gem. BSI-KritisV sind betroffen?	Trinkwasserversorgung
	Welche Anlagentypen gem. BSI-KritisV sind betroffen bzw. könnten betroffen sein? (Nummer und Anlagenbezeichnung)	Gewinnungsanlage

2. Beschreibung der IT-Störung

2.1	Welche Grundwerte der Informations-sicherheit wurden verletzt? (Mehrfachnennungen möglich)	☒ Verfügbarkeit ☒ Integrität ☐ Authentizität ☐ Vertraulichkeit
2.2	Auf welchem/r IT-System / IT-Prozess / IT-Komponente ist was aufgetreten? (Kurzbeschreibung)	Fehlfunktion und Abstürze der PC-gestützten Pumpensteuerung
2.3	Wie ist es aufgetreten?	Konfigurationsdateien des Programms zur Pumpsteuerung wurden von Locky verschlüsselt
2.4	Welche (erfolgreichen) Gegen-maßnahmen wurden eingeleitet?	Locky wurde vom PC entfernt, Neuinstallation beauftragt
2.5	Datum und Zeit, an dem die IT-Störung eingetreten ist	31.03.2016 20:00 Uhr
2.6	Datum und Zeit, an dem die IT-Störung entdeckt wurde	01.04.2016 08:00 Uhr
2.7	Die IT-Störung hält noch an	☒ Ja ☐ Nein – Dauer (dd:hh:mm):
2.8	Wie ist die IT-Störung aufgefallen? (Mehrfachnennungen möglich)	

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

3. Vermutete oder tatsächliche Ursachen

3.1	Physikalischer Schaden (Mehrfachnennungen möglich)	☐ Zerstörung von Geräten ☐ Manipulation von Geräten ☐ Sonstiges:	☐ Diebstahl von Geräten ☐ Verlust von Geräten
3.2	Technisches Versagen (Mehrfachnennungen möglich)	☐ Versagen der Hardware ☐ Software fehlerhaft ☐ Sonstiges:	☐ Überlastung ☐ Fehlverhalten von Systemen
3.3	Organisatorische Ursache (Mehrfachnennungen möglich)	☐ Fehlbedienung ☐ Social Engineering ☐ Sonstiges:	☐ Unautorisierte Nutzung von Ressourcen
3.4	Versagen der genutzten Infrastruktur (Mehrfachnennungen möglich)	☐ Stromausfall ☐ Kühlungsausfall ☐ Sonstiges:	☐ Netzwerkausfall

3.5	Technischer Angriff (Mehrfachnennungen möglich)		
	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:	**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:
	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:	**Missbrauch (Innentäter)** ☐ Weitergabe interner Informationen ☐ Unberechtigtes Erlangen von besonderen Zugriffsrechten, z.B. von Administrationsrechten ☐ Missbräuchliche Nutzung von Berechtigungen (insb. von Zugriffsrechten), z.B. durch Externe über Fernwartungszugänge ☐ 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:**
3.6*	Sonstiges (z. B. CVE, Name der Schadsoftware, weitergehende Informationen, ...)	Locky	

4. Allgemeine Informationen zum informationstechnischen Angriff

☐	Es handelt sich **nicht** um einen informationstechnischen Angriff (dann kein Ausfüllen der Felder 4.1-4.5 notwendig)	
4.1	Angriffsart	☐ Gezielter Angriff ☐ Ungerichteter Angriff ☒ Unbekannt
4.2	Bei mehrfachen Angriffen bitte vermutete Anzahl angeben	
4.3*	Vermutete Motivation (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? (Mehrfachnennungen möglich)	☐ 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.	☒ Unbekannt / keine Angabe ☐ Es wurde keine Strafanzeige gestellt ☐ Strafanzeige wurde gestellt Aktenzeichen: Polizeidienststelle: Bundesland: ☐ Weiterleitung der Meldung an BKA durch BSI ist erwünscht ☐ Täter wurde ermittelt

* Freiwillige Angabe

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? **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.)	☐ Ja, zu einem Ausfall ☒ Ja, zu einer Beeinträchtigung ☐ Nein (dann kein Ausfüllen der Felder 5.6 bis 5.8 notwendig)
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 Ihres Wissens 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**) ☒ 250.000 bis 500.000 (bzw. 50% bis 100%) ☐ 500.000 bis 1.000.000 (bzw. 100% bis 200%) ☐ 1.000.000 bis 5.000.000 (bzw. 200% bis 1000%) ☐ > 5.000.000 Einwohner (bzw. > 1000%) ☐ Es kann keine Aussage gemacht werden
5.4	Wie ist die (potentielle) geographische 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 (potentiell) grenzüberschreitend? **Wenn ja:** Welche Staaten sind / wären ebenfalls betroffen?	☐ Ja ☒ Nein
5.6	Von wann bis wann bestand die Beeinträchtigung / der Ausfall der Funktionsfähigkeit der Kritischen Infrastruktur (also der kritischen Dienstleistungen)?	Von ca. (TT.MM.JJJJ hh:mm): Bis ca. (TT.MM.JJJJ hh:mm): ☒ Auswirkung dauert an
5.7	Wann wurde die Beeinträchtigung / der Ausfall der Funktionsfähigkeit der Kritischen Infrastruktur (also der kritischen Dienstleistungen) festgestellt?	Am (ca.) (TT.MM.JJJJ hh:mm): 01.04.2016 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	

* Freiwillige Angabe