

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)	<input type="checkbox"/> Freiwillige Mitteilung ohne gesetzliche Verpflichtung <input checked="" type="checkbox"/> Erstmeldung gemäß gesetzlicher Verpflichtung BSIG §8b (4) <input type="checkbox"/> Folgemeldung zu IT-Störungsnummer: <input type="checkbox"/> Abschlussmeldung zu IT-Störungsnummer:
1.2	Wie ist Ihre aktuelle Lageeinschätzung?	<input type="checkbox"/> Rot (Ausfall der kritischen Versorgungsdienstleistung auf lokaler, regionaler, nationaler Ebene erwartet bzw. eingetreten) <input checked="" type="checkbox"/> Orange (Beeinträchtigung der kritischen Versorgungsdienstleistung bis hin zum Notbetrieb erwartet bzw. eingetreten) <input type="checkbox"/> Gelb (Verstärkte Auffälligkeiten in der Kritischen Informationsinfrastruktur, aber keine Beeinträchtigung der Versorgungsdienstleistung eingetreten, oder es werden nur geringe Beeinträchtigungen erwartet) <input type="checkbox"/> 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 <input type="checkbox"/> Elektrizität <input type="checkbox"/> Gas <input type="checkbox"/> Mineralöl Ernährung <input type="checkbox"/> Ernährungswirtschaft <input type="checkbox"/> Lebensmittelhandel Finanz- und Versicherungswesen <input type="checkbox"/> Banken <input type="checkbox"/> Börsen <input type="checkbox"/> Versicherungen <input type="checkbox"/> Finanzdienstleister	Wasser <input checked="" type="checkbox"/> Öffentliche Wasserversorgung <input type="checkbox"/> Öffentliche Abwasserbeseitigung Informationstechnik und Telekommunikation <input type="checkbox"/> Informationstechnik <input type="checkbox"/> Telekommunikation
		Gesundheit <input type="checkbox"/> Medizinische Versorgung <input type="checkbox"/> Arzneimittel und Impfstoffe <input type="checkbox"/> Labore Transport und Verkehr <input type="checkbox"/> Luftfahrt <input type="checkbox"/> Seeschifffahrt <input type="checkbox"/> Binnenschifffahrt <input type="checkbox"/> Schienenverkehr <input type="checkbox"/> Straßenverkehr <input type="checkbox"/> 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 Informationssicherheit wurden verletzt? (Mehrfachnennungen möglich)	<input checked="" type="checkbox"/> Verfügbarkeit <input checked="" type="checkbox"/> Integrität <input type="checkbox"/> Authentizität <input type="checkbox"/> 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) Gegenmaßnahmen 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	<input checked="" type="checkbox"/> Ja <input type="checkbox"/> Nein – Dauer (dd:hh:mm):
2.8	Wie ist die IT-Störung aufgefallen? (Mehrfachnennungen möglich)	
	<input checked="" type="checkbox"/> Systemausfall <input checked="" type="checkbox"/> Fehlverhalten von Systemen <input type="checkbox"/> Auswertung von Logfiles <input type="checkbox"/> Systemwartung <input type="checkbox"/> Technisches (Netz-)Monitoring <input type="checkbox"/> Testbetrieb <input type="checkbox"/> Hinweise von Dritten <input type="checkbox"/> Veröffentlichung von gestohlenen Informationen durch Dritte <input type="checkbox"/> Audit, Prüfung, Zertifizierung <input type="checkbox"/> Hinweise des BSI <input type="checkbox"/> Sonstiges:	

3. Vermutete oder tatsächliche Ursachen

3.1	Physikalischer Schaden (Mehrfachnennungen möglich)	<input type="checkbox"/> Zerstörung von Geräten <input type="checkbox"/> Diebstahl von Geräten <input type="checkbox"/> Manipulation von Geräten <input type="checkbox"/> Verlust von Geräten <input type="checkbox"/> Sonstiges:
3.2	Technisches Versagen (Mehrfachnennungen möglich)	<input type="checkbox"/> Versagen der Hardware <input type="checkbox"/> Überlastung <input type="checkbox"/> Software fehlerhaft <input type="checkbox"/> Fehlverhalten von Systemen <input type="checkbox"/> Sonstiges:
3.3	Organisatorische Ursache (Mehrfachnennungen möglich)	<input type="checkbox"/> Fehlbedienung <input type="checkbox"/> Unautorisierte Nutzung von Ressourcen <input type="checkbox"/> Social Engineering <input type="checkbox"/> Sonstiges:
3.4	Versagen der genutzten Infrastruktur (Mehrfachnennungen möglich)	<input type="checkbox"/> Stromausfall <input type="checkbox"/> Netzwerkausfall <input type="checkbox"/> Kühlausfall <input type="checkbox"/> Sonstiges:

3.5 Technischer Angriff (Mehrfachnennungen möglich)		
<p>Ausnutzung von Schwachstellen</p> <input type="checkbox"/> Nutzung von Systemressourcen (Spam-Relay, Botnetz-Client, C&C-Server, Dropzone-Server)	<p>Hacking und Manipulationen</p> <input type="checkbox"/> Webanwendungsbasierte Angriffe, z.B. Drive-by-Exploits	<p>Schadprogramme (Malware)</p> <input checked="" type="checkbox"/> Malware-Infektion, z.B. durch Trojaner, Rootkits zum Zwecke der Kontrollübernahme, der Datenmanipulation oder des Datenabflusses
<input type="checkbox"/> Code Execution <input type="checkbox"/> Protokollschwachstelle <input type="checkbox"/> Privilege Escalation <input type="checkbox"/> Injection-Angriff <input type="checkbox"/> Cross-Site-Scripting <input type="checkbox"/> Cross-Site-Request-Forgery <input type="checkbox"/> Schwache Algorithmen/Schlüssel <input type="checkbox"/> Sonstiges:	<input type="checkbox"/> Angriffe auf Webanwendungen, z.B. SQL-Injection, Buffer Overflow <input type="checkbox"/> Angriffe auf Anwendungen bzw. Dienste wie DNS, SMTP, FTP <input type="checkbox"/> Systematisches Ausprobieren von Passwörtern <input type="checkbox"/> Sonstiges:	<input checked="" type="checkbox"/> Ransomware z.B. Sperren von IT-Systemen zu Erpressungszwecken <input type="checkbox"/> Adware, Scareware z.B. zu Betrugszwecken <input type="checkbox"/> Multifunktionale Malware z.B. Viren, Würmer, Riskware <input type="checkbox"/> Sonstiges:
<p>Gezielte, mehrstufige kombinierte Angriffe (APT-Angriffe)</p> <input checked="" type="checkbox"/> Initialer Angriff per E-Mail <input checked="" type="checkbox"/> Initialer Angriff über Webseiten (Watering hole attack)	<p>Missbrauch (Innentäter)</p> <input type="checkbox"/> Weitergabe interner Informationen <input type="checkbox"/> Unberechtigtes Erlangen von besonderen Zugriffsrechten, z.B. von Administrationsrechten <input type="checkbox"/> Missbräuchliche Nutzung von Berechtigungen (insb. von Zugriffsrechten), z.B. durch Externe über Fernwartungszugänge <input type="checkbox"/> Sonstiges:	<p>Identitätsmissbrauch</p> <input type="checkbox"/> Verschleierung einer Identität <input type="checkbox"/> Diebstahl von Zugangsdaten, z.B. Identitätsdiebstahl, Phishing, Spear-Phishing, Pharming, Skimming <input type="checkbox"/> Diebstahl oder Fälschung von Zertifikaten <input type="checkbox"/> Unrechtmäßige Registrierung von Internetdomänen (Cybersquatting) <input type="checkbox"/> Sonstiges:
<p>Verhinderung von Diensten</p> <input type="checkbox"/> Überflutung, z.B. (D)DoS <input type="checkbox"/> Gezielter Systemabsturz, z.B. Paketfragmentierung <input type="checkbox"/> Sonstiges:		<p>Sonstiges:</p>
<p>3.6* Sonstiges (z. B. CVE, Name der Schadsoftware, weitergehende Informationen, ...)</p>	<p>Locky</p>	

4. Allgemeine Informationen zum informationstechnischen Angriff

<input type="checkbox"/> Es handelt sich nicht um einen informationstechnischen Angriff (dann kein Ausfüllen der Felder 4.1-4.5 notwendig)	
4.1	<p>Angriffsart</p> <input type="checkbox"/> Gezielter Angriff <input type="checkbox"/> Ungerichteter Angriff <input checked="" type="checkbox"/> Unbekannt
4.2	<p>Bei mehrfachen Angriffen bitte vermutete Anzahl angeben</p>
4.3*	<p>Vermutete Motivation (Mehrfachnennungen möglich)</p> <input checked="" type="checkbox"/> Unbekannt <input checked="" type="checkbox"/> Finanziell <input type="checkbox"/> Persönlich <input type="checkbox"/> Politisch <input checked="" type="checkbox"/> Kriminell <input type="checkbox"/> Terroristischer Hintergrund (Pflicht für das BSI zur Weitergabe der Meldung an BKA) <input type="checkbox"/> Nachrichtendienstlicher Hintergrund (Pflicht für das BSI zur Weitergabe der Meldung an BfV) <input type="checkbox"/> Sonstiges:
4.4	<p>Welche Daten sind im Rahmen der bisherigen Analyse der IT-Störung angefallen und können dem BSI zur Verfügung gestellt werden? (Mehrfachnennungen möglich)</p> <input type="checkbox"/> Malware-Samples <input type="checkbox"/> Hashsummen <input type="checkbox"/> Dateinamen <input type="checkbox"/> Signaturen <input type="checkbox"/> Logfiles <input type="checkbox"/> IP-Adressen <input type="checkbox"/> URLs <input checked="" type="checkbox"/> Sonstiges: Keine / unbekannt / Administratoren untersuchen noch
4.5	<p>Strafverfolgung</p> <p>Wenn eine Strafanzeige gestellt wurde und Sie eine Weiterleitung an das BKA wünschen, ergänzen Sie bitte die entsprechenden Detailangaben.</p> <input checked="" type="checkbox"/> Unbekannt / keine Angabe <input type="checkbox"/> Es wurde keine Strafanzeige gestellt <input type="checkbox"/> Strafanzeige wurde gestellt Aktenzeichen: Polizeidienststelle: Bundesland: <input type="checkbox"/> Weiterleitung der Meldung an BKA durch BSI ist erwünscht <input type="checkbox"/> Täter wurde ermittelt

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

5.1	<p>Hat die IT-Störung zu einem Ausfall oder zu einer Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur (also der kritischen Dienstleistungen) geführt?</p> <p>Wenn nein: Welche Umstände oder Gegenmaßnahmen führen dazu, dass es nicht zu einer Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur kommt?</p> <p>(Bsp.: Unabhängige Parallelversorgung, Angreifer wurde vorher aufgehalten, etc.)</p>	<p><input type="checkbox"/> Ja, zu einem Ausfall</p> <p><input checked="" type="checkbox"/> Ja, zu einer Beeinträchtigung</p> <p><input type="checkbox"/> Nein (dann kein Ausfüllen der Felder 5.6 bis 5.8 notwendig)</p>
5.2	<p>Inwiefern ist die Funktionsfähigkeit der Kritischen Infrastruktur (also die Verfügbarkeit der kritischen Dienstleistungen) beeinträchtigt bzw. könnte sie beeinträchtigt werden?</p> <p>(u.a. welche Systeme und Komponenten sind betroffen bzw. könnten betroffen sein?)</p>	<p>Die Wasserpumpe „Mustermündung“ arbeitet unregelmäßig und liefert nur noch einen Bruchteil der im Normalbetrieb gewonnenen Wassermenge.</p>
5.3	<p>Wie viele Personen könnten Ihres Wissens von der Beeinträchtigung / dem Ausfall der Funktionsfähigkeit der Kritischen Infrastruktur betroffen sein?</p>	<p><input type="checkbox"/> < 250.000 Einwohner (bzw. < 50% der in der BSI-KritisV für Ihre Anlage angegebenen Schwelle)</p> <p><input checked="" type="checkbox"/> 250.000 bis 500.000 (bzw. 50% bis 100%)</p> <p><input type="checkbox"/> 500.000 bis 1.000.000 (bzw. 100% bis 200%)</p> <p><input type="checkbox"/> 1.000.000 bis 5.000.000 (bzw. 200% bis 1000%)</p> <p><input type="checkbox"/> > 5.000.000 Einwohner (bzw. > 1000%)</p> <p><input type="checkbox"/> Es kann keine Aussage gemacht werden</p>
5.4	<p>Wie ist die (potentielle) geographische Verbreitung der Beeinträchtigung / des Ausfalls der Funktionsfähigkeit der Kritischen Infrastruktur (also der kritischen Dienstleistungen)?</p> <p>(Stadt, Region, Landkreis, Bundesland, Bundesgebiet)</p>	<p>Musterstadt und umliegender Kreis</p>
5.5	<p>Ist der Vorfall (potentiell) grenzüberschreitend?</p> <p>Wenn ja: Welche Staaten sind / wären ebenfalls betroffen?</p>	<p><input type="checkbox"/> Ja <input checked="" type="checkbox"/> Nein</p>
5.6	<p>Von wann bis wann bestand die Beeinträchtigung / der Ausfall der Funktionsfähigkeit der Kritischen Infrastruktur (also der kritischen Dienstleistungen)?</p>	<p>Von ca. (TT.MM.JJJJ hh:mm):</p> <p>Bis ca. (TT.MM.JJJJ hh:mm):</p> <p><input checked="" type="checkbox"/> Auswirkung dauert an</p>
5.7	<p>Wann wurde die Beeinträchtigung / der Ausfall der Funktionsfähigkeit der Kritischen Infrastruktur (also der kritischen Dienstleistungen) festgestellt?</p>	<p>Am (ca.) (TT.MM.JJJJ hh:mm):</p> <p>01.04.2016 08:00</p>
5.8	<p>Welche Maßnahmen wurden ergriffen, um die Beeinträchtigung/den Ausfall der Funktionsfähigkeit der Kritischen Infrastruktur (also der kritischen Dienstleistung) zu mindern oder zu beheben?</p>	<p>Suche nach Original-Konfigurationsdateien</p>

6. Sonstiges

6.1*	Weiterführende Informationen	
6.2*	Weiterführende Bewertungen	
6.3*	Weiteres	