Der Hessische Ministerpräsident
Volker Bouffier, MdL

HESSEN

Hessische Staatskanzlei · Postfach 31 47 · 65021 Wiesbaden

An die
Betreiber Kritischer Infrastrukturen
in Hessen
(gemäß Verteiler)

ELEKTRONISCHE POST

Wiesbaden, den 10. März 2022

Hinweise für die Betreiber Kritischer Infrastrukturen in Hessen
hier: Lagebild, Informationsaustausch und Meldewesen insbesondere vor dem Hintergrund des Russland-Ukraine-Konflikts

Sehr geehrte Damen und Herren,

nachdem die Hessische Landesregierung zuletzt im Zusammenhang mit der SARS-CoV-2-Pandemie und den Entwicklungen rund um die Variante Omikron / B1.1.529 auf Sie als Betreiber Kritischer Infrastruktur (KRITIS-Betreiber) in Hessen zugekommen ist, wenden wir uns heute vor dem Hintergrund des Russland-Ukraine-Konflikts an Sie.

Zunächst danke ich Ihnen stellvertretend für die gesamte Hessische Landesregierung für Ihren außerordentlichen Einsatz zum Erhalt der Funktions- und Versorgungsfähigkeit der Kritischen Infrastruktur in Hessen auch während der Omikron-Welle. Der bisherige Verlauf zeigt, dass die KRITIS-Betreiber zielführende Maßnahmen ergriffen und damit nicht zuletzt weitreichende Versorgungsausfälle und entsprechende Beeinträchtigungen des Gemeinwesens vermieden haben. Nach derzeitigem Stand scheint der Höhepunkt der Omikron-Welle überschritten zu sein; viele von Ihnen haben uns mitgeteilt, dass eine gewisse Entspannung der Lage eingetreten ist. Gleichwohl ist die Pandemie nicht vorbei – auch wenn sie derzeit in der öffentlichen Wahrnehmung durch andere Themen überlagert wird. Die gemachten Erfahrungen können und sollten wir in die Vorbereitung auf die weiteren Wellen einfließen lassen.

65183 Wiesbaden
Georg-August-Zinn-Straße 1
Telefon (06 11) 32 0
Telefax (06 11) 3211 3708
E-Mail: poststelle@stk.hessen.de
De-Mail: poststelle@stk-hessen.de-mail.de
Internet: www.hessen.de

Gütesiegel Familienfreundlicher Arbeitgeber Land Hessen

Gleichzeitig sind wir gemeinsam nun noch zusätzlich herausgefordert: Neben die Bewältigung der Pandemie ist der kriegerische Konflikt zwischen Russland und der Ukraine getreten, der auch mit Auswirkungen auf die sicherheitspolitische Lage in Deutschland einhergeht.
Wie Sie der allgemeinen Berichterstattung bereits entnehmen konnten, müssen wir für etwaige Implikationen für die Kritische Infrastruktur in Hessen sensibilisiert sein. Hier spielt insbesondere das gesteigerte allgemeine Cyberbedrohungspotenzial eine Rolle.

Grundsätzlich werden die Kampfhandlungen in der Ukraine durch Maßnahmen im Cyberraum flankiert (hybride Kriegsführung). Verstärkte Cyberangriffe können angesichts hoch vernetzter, weltweit verteilter IT-Systeme auch Netzwerke dritter Akteure in Mitleidenschaft ziehen. Gleichzeitig sind auch Spill-Over-Effekte und Kollateralschäden mit Auswirkungen auf Deutschland im Zuge internationaler Betroffenheiten möglich. Somit können Cyberaktivitäten auch gewollte oder zumindest in Kauf genommene schädliche Auswirkungen außerhalb der Ukraine haben. Zudem besteht ein Risiko von Cyberangriffen gegen deutsche Stellen in Reaktion auf Sanktionen.

Vor diesem Hintergrund steht die Hessische Landesregierung eng an der Seite der KRITIS-Betreiber in Hessen, um Sie bei den bevorstehenden Herausforderungen bestmöglich zu unterstützen. Wichtigstes Anliegen ist die Reduzierung der Verwundbarkeit durch Schutzmaßnahmen, also die Vermeidung von Beeinträchtigungen bzw. Ausfällen, sowie eine umfassende Vorbereitung auf (unvermeidbare) Beeinträchtigungen / Ausfälle. Daneben geht es um eine Verzahnung im Krisenmanagement im Falle von eingetretenen Störungen.

Informationen zur Kritischen Infrastruktur werden wir auch weiterhin im Ihnen bekannten Internetauftritt der Landesregierung (unter www.hessen.de/KRITIS) bereitstellen, sobald dies erforderlich wird.

Daneben möchte ich Sie gerne auf folgende Punkte aufmerksam machen:

1) Lagebild

Wie bereits im Zuge der Omikron-Welle erfolgreich praktiziert, erstellen wir zusammen mit dem Bund ein regelmäßiges Lagebild-KRITIS (zunächst wöchentlich). Hierfür sind wir

(weiterhin) auf Ihre Informationen angewiesen. Wir werden diesbezüglich kurzfristig auf Sie bzw. Ihre verbandlichen Vertretungen zukommen.

Hierbei geht es in erster Linie um eine (qualitative) Einschätzung zu akuten Beeinträchtigungen / Einschränkungen der kritischen Dienstleistungen, zu einem prognostischen Ausblick hinsichtlich Einschränkungen in den kommenden Tagen, zu den betreiberseitig ergriffenen Maßnahmen (um Einschränkungen vorzubeugen oder entgegenzuwirken) sowie zu einem etwaigen behördlichen Unterstützungsbedarf.

Für den Fall, dass eine Beeinträchtigung der Erbringung der kritischen Dienstleistungen Ihrer Organisation droht, informieren Sie uns im Sinne unseres gemeinschaftlichen Agierens in Hessen bitte auch zwischen den regelmäßigen Abfragezeitpunkten.

Sie erreichen uns in allen KRITIS-Angelegenheiten unter der E-Mail-Adresse
kritis@stk.hessen.de.

2) Informationsaustausch bzgl. IT-Sicherheitsaspekten

Bitte überprüfen Sie Ihr Business Continuity Management (BCM) und Ihr Krisenmanagement mit Blick auf die aktuellen Risiken und die allgemeine Gefahrenlage, insbesondere die stark erhöhte Wahrscheinlichkeit von Cyberangriffen. Grundsätzlich haben die allgemein bekannten generellen und branchenspezifischen Regelwerke, Leitfäden und Schutzkonzepte weiterhin Gültigkeit. Beispielhaft sei auf das Basisschutzkonzept KRITIS verwiesen, auf die Empfehlungen zum Selbstschutz, die verschiedenen Checklisten zur Notfallplanung, die BSI-Sicherheitsstandards und das IT-Grundschutzkompendium.

In diesem Zusammenhang weise ich auch gerne noch einmal auf die Prüfpunkte aus meinem Schreiben vom Dezember 2021 hin (z. B. die Sicherstellung der Erreichbarkeiten von Schlüsselpersonal, die Klärung von Zuständigkeiten für den Notfall, die Schulung der Mitarbeitenden in Notfallkonzepten oder die Vorbereitungen zur internen und externen Krisenkommunikation).

Zusätzlich zu den bekannten und eingespielten Informations- und Austauschkanälen bieten wir Ihnen als Betreiber Kritischer Infrastruktur in Hessen für den Bereich der IT-

Security an, sich für den Warn- und Informationsdienst des Hessen CyberCompetence-Center (Hessen3C) zu registrieren.

Über den Warn- und Informationsdienst erhalten Sie 24/7-kritische Meldungen zur IT- und Cybersicherheit und ggfs. Zugang zu nichtöffentlichen Informationen.

Hierzu senden Sie bitte eine E-Mail mit folgenden Angaben

- Firmenangaben (Name des Unternehmens, Anschrift, ggf. Hauptsitz)
- Sektor*
- Branche*
- Kritische Dienstleistung*
  [*) gemäß KRITIS-Übersichtsliste Hessen – siehe www.hessen.de/KRITIS]
- Umfang der Versorgungsleistung (z. B. ungefähr versorgte Einwohner auf volle 10.000 gerundet)
- Kontaktadressen: Funktionspostfach und Telefonnummer Ihres Krisenmanagements, Sicherheitsbeauftragten o. ä.
- unterschriebene TLP-Verpflichtungserklärung (Scan) (s. u.)

und dem Betreff

[Ticket#2022030430000256] Registrierung KRITIS-Betreiber Hessen

an die E-Mail-Adresse

cert@hessen3c.hessen.de.

Um Ihnen ggfs. auch nichtöffentliche Informationen zur Verfügung stellen zu können, benötigt der Warn- und Informationsdienst des Hessen CyberCompetenceCenter (Hessen3C) zwingend eine unterschriebene TLP-Verpflichtungserklärung

Bitte beachten Sie, dass die Verpflichtungen gemäß BSIG auch bei einer Zusammenarbeit mit dem Hessen CyberCompetenceCenter weiterbestehen.

Daneben weise ich Sie auch gerne noch einmal auf die Kategorie IT-Sicherheit in der App „hessenWARN“ hin.

Selbstverständlich hoffen wir derzeit alle auf Deeskalation. Dennoch müssen wir uns im Sinne des Vorbereitet seins bestmöglich auf aktuelle Risiken, insbesondere etwaige Cyberangriffsszenarien, und mögliche Krisenlagen einstellen.

Ich darf mich abschließend noch einmal für Ihr Engagement und Ihren Einsatz bedanken und versichere Ihnen, dass der Hessischen Landesregierung der Erhalt der Funktions- und Versorgungsfähigkeit der Kritischen Infrastruktur in Hessen ein besonderes Anliegen ist.

Mit freundlichen Grüßen

(Volker Bouffier)

Anlage