Deutscher Bundestag **Drucksache 19/24090**

19. Wahlperiode 05.11.2020

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Joana Cotar, Uwe Schulz, Dr. Michael Espendiller und der Fraktion der AfD
– Drucksache 19/23552 –

Unzureichende IT-Sicherheit Citrix

Vorbemerkung der Fragesteller

In deutschen Unternehmen und Organisationen werden trotz jahrelanger Bemühungen der Bundesregierung, der IT-Sicherheit eine zentrale Bedeutung zukommen zu lassen, immer noch fahrlässig ungesicherte Systeme betrieben (https://fm4.orf.at/stories/3007764/). Das Resultat sind unter anderem unwiderruflich verlorene Daten, Datenleaks, Erpressungen, Ausfall systemrelevanter Infrastruktur und im schlimmsten Fall sogar Todesfälle (https://www.tagesspiegel.de/gesellschaft/panorama/it-ausfall-im-krankenhaus-frau-nach-hackerangriff-auf-duesseldorfer-uni-klinik-verstorben/26195960.html).

Um dem entgegenzuwirken, versucht das CERT (Computer Emergency Response Team) des Bundesministeriums des Innern, für Bau und Heimat (BMI) gerade, „die letzten immer noch ungesicherten Citrix-Maschinen postalisch zu kontaktieren. Eine unbekannte Zahl spät gesicherter Systeme ist seit dem Frühjahr mit Hintertüren versehen. Für die F5-Gateways gilt dasselbe seit Ende Juli."

Hier besteht nach Ansicht der Fragesteller akuter Handlungsbedarf, um das Schadenspotential auf ein Minimum zu reduzieren.

1. Wie häufig haben Bundesbehörden Betreiber von unzureichend gesicherten IT-Komponenten postalisch kontaktiert?

Eine postalische Kontaktaufnahme zu Betreibern verwundbarer oder kompromittierter Systeme findet seitens des hier zuständigen Bundesamtes für Sicherheit in der Informationstechnik (BSI) grundsätzlich nicht statt. Üblicherweise liegen dem BSI nur die IP-Adressen der jeweiligen Systeme vor, die Identität der jeweiligen Kunden ist in der Regel nur dem zugehörigen Internet-Service-Provider (ISP) bekannt.

Das BSI übermittelt täglich auf elektronischem Weg eine sechsstellige Anzahl von Warnmeldungen an die ISP, in denen diese über verwundbare bzw. bereits kompromittierte Systeme ihrer Kunden in Deutschland in Kenntnis gesetzt wer-

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern, für Bau und Heimat vom 4. November 2020 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

den. Diese Warnungen sind mit der Aufforderung verbunden, sie an die jeweils betroffenen Kunden weiterzuleiten.

Im Rahmen der auch nach Monaten weiterhin verwundbaren Citrix-Systeme hat das BSI manuell die Identität von Betroffenen erhoben und 134 Betreiber kompromittierbarer IT-Systeme postalisch informiert. Dies erfolgte aufgrund der besonderen Umstände des Einzelfalles.

2. Versucht die Bundesregierung, neben einer Kontaktaufnahme per Post andere Möglichkeiten wie Fax, telefonische, persönliche Kontaktaufnahme zu nutzen?

Im Januar 2020 waren in Deutschland über 5.000 IT-Systeme über die Schwachstelle CVE-2019-19781 angreifbar. Das BSI hat die ISP über das o. g. Verfahren unverzüglich über die betroffenen Systeme informiert. Die Zahl der verwundbaren Systeme ist daraufhin stark zurückgegangen.

Im Oktober 2020 hat sich das BSI per Brief an die Geschäftsführungen derjenigen Betreiber gewandt, deren IT-Systeme weiterhin über die Schwachstelle CVE-2019-19781 angreifbar waren. In diesem speziellen Fall war eine Identifizierung der Betreiber möglich, da die Domain-Namen der betroffenen Systeme bekannt waren. Der Weg per Brief an die Geschäftsführungen wurde gewählt, da der übliche Weg über die ISP in diesen Fällen offensichtlich nicht zum Erfolg geführt hatte. Nach der Ansprache per Brief schlossen etwa die Hälfte der Angeschriebenen die Lücke in ihren Systemen. Die andere Hälfte der Systeme war weiterhin angreifbar. Daraufhin erfolgte durch das BSI stichprobenartig die telefonische Kontaktaufnahme mit den jeweiligen Geschäftsführungen einiger der betroffenen IT-Systeme, um die Gründe für deren Nicht-Tätigwerden in Erfahrung zu bringen.

3. Welche IT-Systeme sind nach Kenntnis der Bundesregierung von den Angriffen betroffen (bitte die IT-Systeme auflisten)?

Folgende Systeme sind von der Schwachstelle CVE-2019-19781 betroffen:

- Citrix ADC und Citrix Gateway Version 13.0 vor 13.0.47.24
- NetScaler ADC und NetScaler Gateway Version 12.1 vor 12.1.55.18
- NetScaler ADC und NetScaler Gateway Version 12.0 vor 12.0.63.13
- NetScaler ADC und NetScaler Gateway Version 11.1 vor 11.1.63.15
- NetScaler ADC und NetScaler Gateway Version 10.5 vor 10.5.70.12
- Citrix SD-WAN WANOP appliance Modelle 4000-WO, 4100-WO, 5000-WO, und 5100-WO vor Version 10.2.6b und 11.0.3b.

4. Wie hoch schätzt die Bundesregierung die Zahl der in Deutschland zu spät gesicherten Citrix-Systeme, welche mittlerweile mit Hintertüren versehen sind oder höchstwahrscheinlich versehen werden könnten?

Der Bundesregierung liegen keine verlässlichen Zahlen zu derart betroffenen Citrix- Systemen vor. Allerdings wurde bei mehreren Angriffen in den letzten Monaten ein bereits vorab durch die Tätergruppierungen installierte Remotezugang genutzt. Es handelte sich dabei nicht um eine Funktion der Software Citrix. Bei allen Systemen, die noch im Januar verwundbar waren, ist daher davon auszugehen, dass dort ebenfalls ein nachträglicher Remotezugang durch die Tätergruppierungen installiert wurde. Dies entspricht oft dem Vorgehen der

Tätergruppierungen, sich Zugang zu einem System zu verschaffen, diesen aber erst später zu nutzen. Es liegen aktuell keine Erkenntnisse vor, ob die Unternehmen auch nach dem Installieren des Patches das System auf weiter zusätzlich eingefügte Remotezugänge geprüft haben oder andere Schutzmaßnahmen getroffen haben. Das BSI hat diese Problematik mit seinen Sicherheitswarnungen an die Unternehmen adressiert.

5. Hat die Bundesregierung Grund zu der Annahme, dass von den weiterhin ungesichert betriebenen Citrix-Systemen direkt oder indirekt kritische Infrastruktur (KRITIS) betroffen ist?

   Wenn nein, warum nicht?

Nein, bei allen dem BSI bekannten KRITIS-Zuordnungen wurden die Systeme gepatcht. Das Melde- und Informationssystem zwischen BSI und KRITIS-Betreibern ist etabliert und hat sich bewährt.

6. Sieht die Bundesregierung legislativen Handlungsbedarf, um die Sicherheit der IT-Systemlandschaft generell zu verbessern, und wenn ja, welche Initiativen plant die Bundesregierung diesbezüglich?

Die Bundesregierung sieht als zentrale legislative Maßnahme zur Verbesserung der IT-Sicherheit in dieser Legislaturperiode das IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0) vor. Bei diesem Gesetz handelt es sich um die Fortschreibung des IT-Sicherheitsgesetzes aus dem Jahr 2015. Das IT-SiG 2.0 ist derzeit in der Ressortabstimmung.

Gesamtherstellung: H. Heenemann GmbH & Co. KG, Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333