KISTERS AG
Pascalstraße 8+10
52076 Aachen
Germany
Tel. +49 2408 9385 -0
Fax +49 2408 9385 -555
E-mail: info@kisters.de
Internet: https://www.kisters.de

KISTERS AG

KISTERS AG · Pascalstraße 8+10 · 52076 Aachen · Germany

KISTERS Geschäftspartner
z.H. Datenschutzbeauftragte

Unser Zeichen
hjs
Ansprechpartner
Dr. Heinz-Josef Schlebusch
Telefon
+49 2408 9385 -226
E-Mail
schlebusch@kisters.de

Datum
17. Nov. 2021

Sehr geehrte Damen und Herren,

Sie sind uns als Datenschutzbeauftragte für einen oder mehrere unserer Geschäftspartner benannt. Zur Wahrung unserer Informationspflicht als Auftragsverarbeiter unterrichten wir Sie hiermit über einen möglichen Datenschutzvorfall im Zusammenhang mit dem Cyberangriff auf die KISTERS AG.

1. Art der Meldung (Art. 33 Abs. 4)
Neumeldung

2. Auftragsverarbeiter (Art. 4 Nr. 8)
Name: KISTERS AG
Straße: Pascalstraße 8+10
PLZ: 52076 Aachen
Telefon: +49 2408 9385-0
E-Mail: info@kisters.de

3. Anlaufstelle für weitere Informationen (Art. 33 Abs. 3 lit. b)
Datenschutzbeauftragter
Name: Dr. Heinz-Josef Schlebusch
Straße: Pascalstraße 8+10
PLZ: 52076 Aachen
Telefon: +49 172 7181 829
E-Mail: datenschutz@kisters.de

4. Bekanntwerden der Verletzung des Schutzes personenbezogener Daten
In der Nacht zum 11. Nov. 2021 wurde die KISTERS AG das Ziel eines Malware-Angriffs. Der vermutliche Zeitraum der Verletzung des Schutzes personenbezogener Daten ist 10. Nov. 2021, zwischen 21:00h und 23:00h.

Zur Untersuchung des Vorfalls wurden unverzüglich externe IT-Sicherheitsexpert:innen hinzugezogen. Im Rahmen der weiterhin laufenden forensischen Untersuchungen haben sich gestern, am **16.11.2021**, Hinweise ergeben, dass auch personenbezogene Daten unserer Auftraggeber, die wir im Rahmen unserer Dienstleistungen als Auftragsverarbeiter auf unseren IT-Systemen verarbeiten oder gespeichert haben, von der Verletzung des Schutzes personenbezogener Daten betroffen sein könnten.

5. Beschreibung der Verletzung des Schutzes personenbezogener Daten
Art der Verletzung des Schutzes personenbezogener Daten (Art. 33 Abs. 3 lit. a, Art. 4 Nr. 12)
Antwort: Unbefugter Zugang, Verlust
Erläuterung: Nach aktuellem Stand der Ermittlungen kann nicht ausgeschlossen werden, dass es zu einem unbefugten Zugang und ggfls. auch zu Verlusten von Datendateien unserer Auftraggeber gekommen ist, die personenbezogene Daten enthalten. Ebenfalls kann derzeit nicht ausgeschlossen werden, dass diese Daten durch die Angreifer-Gruppe gelöscht oder heruntergeladen worden sind.
Wie kam es zu der Verletzung des Schutzes personenbezogener Daten?
Antwort: Hackerangriff (Virus/Trojaner/Phishing)
Erläuterung: Nach aktuellem Kenntnisstand kann derzeit noch keine Aussage dazu getroffen werden, wie sich die Angreifer-Gruppe Zugang verschafft hat.
Wer oder was hat die Verletzung des Schutzes personenbezogener Daten ausgelöst?
Antwort: Person mit Schädigungsabsicht

6. Beschreibung der betroffenen Personen und Daten
Kategorien betroffener Personen (Art. 33 Abs. 3 lit. a)
Antwort: Personen, deren personenbezogene Daten im Rahmen der Bereitstellung und Durchführung unserer Dienstleistungen auf KISTERS IT-Systemen verarbeitet oder gespeichert werden, und für die unsere Auftraggeber Verantwortliche im Sinne der DS-GVO (Art. 4 Nr. 7) sind:

- Daten aus produktiven KISTERScloud-Systemen, die für unsere Auftraggeber als SaaS- oder ASP-Lösungen in unserem Rechenzentrum betrieben werden;
- Daten aus Systemabbildern, Datenbankdumps, Protokolldateien o.ä., die zum Zweck der Systemanalyse oder Fehlerbehebung im Rahmen unserer Consulting- oder Supportservices von unseren Auftraggebern an uns übermittelt wurden;
- Daten, die uns im Rahmen unseres Supportservices von unseren Auftraggebern über unsere Ticketsysteme oder E-Mail übermittelt wurden.

Kategorien betroffener Daten (Art. 33 Abs. 3 lit. a)
Antwort: Die Kategorien der betroffenen Daten sind abhängig von der genutzten Fachanwendung und der individuellen Nutzung durch unsere Auftraggeber.
Ungefähre Zahl betroffener Personen (Art. 33 Abs. 3 lit. a)
Antwort: Nach aktuellem Kenntnisstand kann noch keine Anzahl genannt werden.
Ungefähre Zahl betroffener Datensätze (Art. 33 Abs. 3 lit. a)
Antwort: Nach aktuellem Kenntnisstand kann noch keine Anzahl genannt werden.

7. Folgen der Verletzung des Schutzes personenbezogener Daten
Welche Folgen hat die Verletzung des Schutzes personenbezogener Daten wahrscheinlich für die betroffenen Personen (Art. 33 Abs. 3 lit. c) ?

Antwort: Identitätsdiebstahl, Betrug, Verlust der Kontrolle ihrer personenbezogenen Daten
Erläuterung: Nach derzeitigem Sachstand ist die Verletzung der Integrität und der Vertraulichkeit der betroffenen personenbezogenen Daten möglich. Weitere Erläuterungen sind derzeit noch nicht möglich.
Welches Risiko für die Rechte und Freiheiten betroffener Personen besteht nach aktuellem Kenntnisstand voraussichtlich (Art. 33 Abs. 3 lit. c)?
Antwort: Risiko
Erläuterung: Die Schwere der möglichen Folgen für Betroffene wird hängt von den Kategorien der in den betroffenen Fachanwendungen verarbeiteten oder gespeicherten Daten ab. Eine weitergehende Risikoabschätzung kann nur durch die Verantwortlichen durchgeführt werden.

8. Maßnahmen zur Behebung oder Abmilderung der Verletzung des Schutzes personenbezogener Daten
Welche Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten hat der Auftragsverarbeiter ergriffen bzw. schlägt er vor (Art. 33 Abs. 3 lit. d)?
Antwort: Die gesamte KISTERS IT Infrastruktur wurde vom öffentlichen Netz getrennt. Derzeit sind noch große Teile der IT-Infrastruktur durch die Angreifer-Gruppe verschlüsselt, weswegen eine weitere Behebung der Verletzung des Schutzes personenbezogener Daten noch nicht vorgenommen werden kann.
KISTERS hat nach Kenntnis über den Angriff einen qualifizierten APT-Response-Dienstleister nach BSI beauftragt, um den Sachverhalt digital forensisch aufzuarbeiten. Dazu steht KISTERS mit dem Dienstleister und Datenschutzbeauftragten im engen Austausch. Der Dienstleister ist seit dem 12. Nov. 2021 bei KISTERS vor Ort, um Datensicherungen und Auswertungen durchzuführen. Eine Auswertung von Log- und Metadaten sowie weitere Protokolle und Aufzeichnungen, die den Angriff rekonstruieren könnten, liegt derzeit noch nicht vor. Als Gegenmaßnahme und Aufklärung möchte KISTERS wie bereits zuvor erklärt eine vollständige digital forensische Untersuchung durchführen.
KISTERS steht ebenfalls im Austausch mit den Strafverfolgungsbehörden und hat gegen den Cyber-Angriff Strafanzeige gestellt.
Über die derzeit verfügbaren Informationskanäle wurden bereits Kunden, Interessenten und Geschäftspartner über den Cyber-Angriff benachrichtigt.
Zusätzlich wurde eine temporäre Webseite mit aktueller Information und entsprechenden Hinweisen aufgesetzt (www.kisters.de), über die wir alle interessierten Parteien weiterhin informieren.

Mit freundlichen Grüßen,

Dr. Heinz-Josef Schlebusch
CISO & DSB, KISTERS Gruppe