Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum BSI

SCHWACHSTELLE | GEFÄHRDUNG | **VORFALL** | IT-ASSETS

Cybersicherheitsvorfall bei einem Remote-Screen-Sharing-Anbieter

CSW-Nr. 2024-213655-1032, Version 1.0, 05.02.2024

IT-Bedrohungslage*: 2 / Gelb

Achtung: Für die schriftliche und mündliche Weitergabe dieses Dokumentes und der darin enthaltenen Informationen gelten gemäß dem Traffic Light Protokoll (TLP) die folgenden Einschränkungen:

TLP:CLEAR: Unbegrenzte Weitergabe

Abgesehen von urheberrechtlichen Aspekten, die das TLP explizit nicht adressiert, dürfen Informationen der Stufe TLP:CLEAR ohne Einschränkungen frei weitergegeben werden.

Das Dokument ist durch den Empfänger entsprechend den vereinbarten „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP“ zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten. Weitere Informationen zum TLP finden Sie am Ende dieses Dokumentes.

Sachverhalt

Die AnyDesk Software GmbH – Hersteller der gleichnamigen und weit verbreiteten Software für Fernzugriff und Screensharing – veröffentlichte eine Pressemitteilung zu einem Angriff mit erfolgter Kompromittierung interner Systeme [ANY2024]. Das BSI steht mit dem Unternehmen in Kontakt und kann den Vorfall bestätigen.

Öffentliche Quellen berichten darüber, dass im Zuge dieser Kompromittierung auch Quellcode sowie Zertifikate zum Signieren der Software abgeflossen seien [BLEEP2024]. AnyDesk hat die Bereinigung und Wiederherstellung unmittelbar gemeinsam mit einem Dienstleister durchgeführt. Im Rahmen dessen wurden Zertifikate zurückgezogen und Updates bereitgestellt, durch die die Zertifikate bei den Endnutzern ausgetauscht werden. Hierbei wird nach Informationen von der Anydesk Software GmbH an das BSI u.a. das folgende Zertifikat ausgetauscht:

- Zertifikat-Seriennummer: 0DBF152DEAF0B981A8A938D53F769DB8

AnyDesk hat den Quellcode zudem gründlich überprüft und konnte keine Manipulation feststellen. Die AnyDesk Software GmbH äußerte gegenüber dem BSI, dass das Unternehmen derzeit keine positive Kenntnis einer Kompromittierung von Nutzerdaten hat. AnyDesk hat jedoch aus Gründen der Vorsicht einen Reset der Passwörter des Kundenportals my.anydesk.com erzwungen.

* 1 / Grau: Die IT-Bedrohungslage ist ohne wesentliche Auffälligkeiten auf anhaltend hohem Niveau.
2 / Gelb IT-Bedrohungslage mit verstärkter Beobachtung von Auffälligkeiten unter temporärer Beeinträchtigung des Regelbetriebs.
3 / Orange Die IT-Bedrohungslage ist geschäftskritisch. Massive Beeinträchtigung des Regelbetriebs.
4 / Rot Die IT-Bedrohungslage ist extrem kritisch. Ausfall vieler Dienste, der Regelbetrieb kann nicht aufrecht erhalten werden.

Bewertung

Nach Einschätzung des BSI besteht durch den möglichen Abfluss des Quellcodes sowie der Zertifikate die Gefahr, dass diese Informationen für weiterführende Angriffe auf Kunden des Anbieters genutzt werden könnten. In diesem Kontext sind unter anderem Man-in-the-Middle- sowie Supply-Chain-Angriffe denkbar. Insbesondere durch die womöglich abgeflossenen Zertifikate könnten diese unbemerkt bleiben oder im schlimmsten Fall bereits erfolgte Angriffe unentdeckt geblieben sein. Durch die vom Betreiber umgesetzten Maßnahmen wird das aktuelle Gefährdungspotenzial erheblich reduziert. Dennoch ist nicht auszuschließen, dass schädliche Versionen der Software, die mit dem kompromittierten Zertifikat signiert sind, durch Angreifer auf Dritt-Seiten angeboten oder gezielt an Kunden gesandt werden.

Im Unternehmenskontext wird die Anwendung oft mit privilegierten Rechten verwendet, wodurch sich ein besonderes Gefährdungspotenzial eröffnet.

Mögliche Auswirkungen auf Kritische Infrastrukturen inkl. Verwaltung

Der geschilderte Vorfall kann in ähnlicher Art auch Kritische Infrastrukturen treffen und die dargestellten Konsequenzen haben.

Empfehlungen an IT-Sicherheitsverantwortliche

Das BSI empfiehlt einen vorsichtigen Umgang mit der Software, insbesondere bei Updates oder dauerhaft offenen Verbindungen. Darüber hinaus sollte der Empfehlung des Herstellers Folge geleistet werden, die jeweils aktuellste Version mit dem neuen Zertifikat einzuspielen. Updates sollten ausschließlich über die Update-Funktion innerhalb der Software oder über die Website des Herstellers bezogen werden.

Darüber hinaus sollten Mitarbeitende (vor allem solche, die schwerpunktmäßig in Kontakt mit dem Unternehmen oder der Software stehen) im eigenen Unternehmen sensibilisiert werden, verbunden mit dem Hinweis, dass Software niemals aus unsicheren Quellen bezogen werden sollte [BSI2024]. Der Hersteller empfiehlt außerdem einen vorsorglichen Passwortwechsel, insbesondere wenn die bei AnyDesk verwendeten Zugangsdaten auch bei anderen Diensten genutzt werden.

Für Fragen seitens der Kunden hat die AnyDesk Software GmbH eine Hotline eingerichtet, die über die E-Mail-Adresse hotline@anydesk.com oder die Telefonnummer +49 711 939 64 381 erreichbar ist.

Links

[ANY2024] AnyDesk Incident Response 2-2-2024:
https://anydesk.com/en/public-statement

[BLEEP2024] AnyDesk says hackers breached its production servers, reset passwords:
https://www.bleepingcomputer.com/news/security/anydesk-says-hackers-breached-its-production-servers-reset-passwords/

[BSI2024] BSI IT-Grundschutz: ORP.3 Sensibilisierung und Schulung zur Informationssicherheit:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/02_ORP_Organisation_und_Personal/ORP_3_Sensibilisierung_und_Schulung_Editon_2023.pdf

Anlagen

Kontakt

Bitte wenden Sie sich bei allen Rückfragen zu diesem Dokument an denjenigen Kontakt, der Ihnen das Dokument zugesendet hat. Dadurch bleibt der Informationsfluss kanalisiert. Die Single Points of Contact (SPOCs), welche das Dokument direkt vom Nationalen IT-Lagezentrum des BSI erhalten haben, können sich direkt an die bekannten Kontaktdaten des Nationalen IT-Lagezentrums im BSI wenden.

Erklärungen zum Traffic Light Protokoll (TLP)

Dieses Dokument und die darin enthaltenen Informationen sind gemäß dem TLP eingestuft:

1) Was ist das Traffic Light Protokoll?

Das vom BSI verwendete TLP basiert auf der Definition der TLP Version 2.0 des „Forum of Incident Response and Security Team“ (FIRST). Es dient der Schaffung von Vertrauen in Bezug auf den Schutz ausgetauschter Informationen durch Regelungen der Weitergabe. Eine unbefugte Weitergabe kann eine Verletzung der Vertraulichkeit, eine Rufschädigung, eine Beeinträchtigung der Geschäftstätigkeit oder datenschutzrechtliche Belange zur Folge haben. Im Zweifelsfall ist immer in Absprache mit dem Informationsersteller zu handeln.

2) Welche Einstufungen existieren?

- **TLP:CLEAR: Unbegrenzte Weitergabe**
  Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:CLEAR ohne Einschränkungen frei weitergegeben werden.

- **TLP:GREEN: Organisationsübergreifende Weitergabe**
  Informationen dieser Stufe dürfen innerhalb der Organisationen und an deren Partner weitergegeben werden. Die Informationen dürfen jedoch nicht veröffentlicht werden. Eine Weitergabe von den Partnerorganisationen an weitere Personen oder Organisationen ist solange zulässig, wie diese weiteren Empfänger derselben Nutzergruppe (bspw. Angehörige der Cybersecurity-Community) angehören.

- **TLP:AMBER: Eingeschränkte interne und organisationsübergreifende Weitergabe**
  Der Empfänger darf die Informationen, welche als TLP:AMBER gekennzeichnet sind, an seine Partner weitergeben, soweit diese die Informationen zur Schadensreduktion oder dem eigenen Schutz benötigen. Eine Weitergabe von den Partnern an Dritte ist nicht erlaubt und auch innerhalb der Partnerorganisationen gilt das Prinzip „Kenntnis nur, wenn nötig“. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen. Diese müssen eingehalten werden.

    TLP:AMBER+STRICT: Eingeschränkte interne Weitergabe
    Die Einstufung von Informationen als TLP:AMBER+STRICT beschränkt die Weitergabe ausschließlich auf die Organisation des Empfängers. Jegliche Weitergabe darüber hinaus ist untersagt. Es gilt „Kenntnis nur, wenn nötig“. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen. Diese müssen eingehalten werden.

- **TLP:RED: Persönlich, nur für benannte Empfänger**
  Informationen dieser Stufe sind auf den Kreis der Anwesenden in einer Besprechung oder Video-/Audiokonferenz bzw. auf die direkten Empfänger bei schriftlicher Korrespondenz beschränkt. Eine Weitergabe ist untersagt. TLP:RED eingestufte Informationen sollten möglichst mündlich oder persönlich übergeben werden.

3) Was mache ich, wenn ich das Dokument an jemanden außerhalb des im TLP vorgegebenen Informationsverbundes weitergeben will?

Sollte eine Weitergabe an einen nicht durch die Einstufung genehmigten Empfängerkreis notwendig werden, so ist diese vor einer eventuellen Weitergabe durch den Informationsersteller nachvollziehbar zu genehmigen. Bei ausnahmsweiser Weitergabe im Rahmen einer bestehenden gesetzlichen Verpflichtung ist der Informationsersteller – nach Möglichkeit vorab – zu informieren.

4) Was passiert, wenn ich die Einstufung nicht beachte?

Bei Verstoß gegen die Regeln zur Weitergabe von Informationen erhält der Verpflichtete zukünftig nur noch TLP:CLEAR eingestufte Informationen aus dem Kreis der Verpflichteten.

Hinweis zu Upload-, Prüf- und Übersetzungsdiensten

TLP-eingestufte Dokumente (außer TLP:CLEAR) dürfen nicht auf Plattformen Dritter (wie Virustotal, Übersetzer, etc.) hochgeladen werden, da die Dokumente dort ggf. Dritten zugänglich gemacht werden.