Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

**Melde- und Analysestelle
Informationssicherung MELANI**

Phishing-Attacken auf Online Datenaustausch - und Kollaborationsplattformen

02.10.2018 - Viele Firmen erlauben ihren Angestellten, Dokumente online zu teilen und sogar auf ganze Bürosysteme online zuzugreifen. Manchmal reicht nur ein Passwort, um Zugriff auf ein E-Mail-Konto, aber auch auf diverse andere Dokumente zu erhalten. Es ist deshalb nicht verwunderlich, dass diese Zugangsdaten von grossem Interesse für Phishing-Angriffe sind. Das Kompromittieren eines ersten Kontos wird daher oft als weiterführender Angriffsvektor gegen die anderen Mitarbeitenden verwendet.

In den letzten Monaten hat MELANI Meldungen zu zahlreichen Phishing-Attacken erhalten, welche solche Plattformen imitieren und versuchen, an Zugangsdaten zu gelangen. Zum Beispiel werden die Webseiten von Microsoft Office 365 oder OneDrive nachgebaut. Die Qualität und die Art der E-Mails unterscheiden sich stark. Bei gewissen E-Mails wird der Empfänger gebeten sich zu identifizieren, um ein Problem mit seinem Konto zu lösen, oder aber aufgefordert, ein mit ihm geteiltes Dokument anzuschauen. In allen Fällen wird der Empfänger auf eine Phishing-Seite weitergeleitet, welche die Seite des Anbieters imitiert; dort sollen der Benutzername und das Passwort angegeben werden.

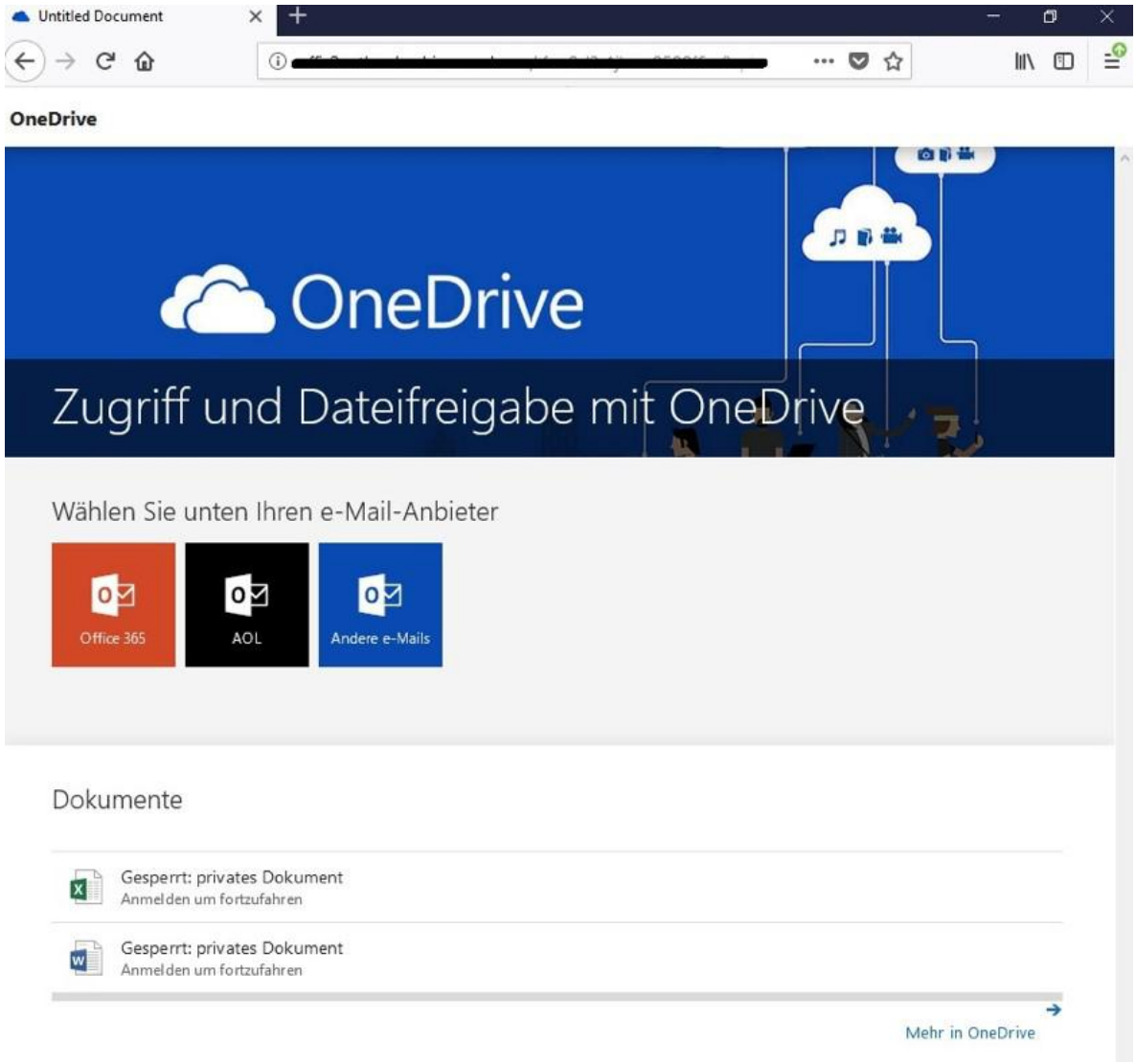

Image 1: Beispiel einer Phishing-Seite, welche OneDrive imitiert

Sobald die Kriminellen Zugang zum Konto haben, können sie prinzipiell dieselben Einstellungen vornehmen wie der Konto-Inhaber:

- Eine E-Mail-Weiterleitung einrichten, sodass sie Zugang zur gesamten Korrespondenz der geschädigten Person haben. Die Weiterleitung erfolgt oft mittels Kopie, so dass dies für den Konto-Inhaber nicht erkennbar ist.
- Wenn das E-Mail-Konto der Plattform als Rücksetz-E-Mail-Adresse für weitere Dienste verwendet wird, könnte ein Angreifer entsprechende Passwörter zurücksetzen lassen und so Zugang zu weiteren Diensten gewinnen.
- Angreifer können sich Zugang zu weiteren Dokumenten verschaffen, soweit die Rechte des Benutzers dies zulassen. Sie können aber auch andere Benutzer im Namen ihres Opfers für die Freigabe von Dokumenten anfragen. Da diese annehmen, dass dies von einem Firmenkollegen geschieht, werden sie diesem Wunsch oft nachkommen.

Für die Kriminellen sind diese Zugangsdaten oft eine Goldmine, welche ihnen erlauben, relevante Informationen, wie beispielsweise Geschäftsbeziehungen, zu bearbeitende Fälle, Struktur und Organigramme des Unternehmens, für einen massgeschneiderten Betrugsversuch zu sammeln. Ebenfalls kann nicht ausgeschlossen werden, dass solche Informationen zur Wirtschaftsspionage benutzt oder weiterverkauft werden.

Sobald ein Konto kompromittiert ist, können alle Kontakte der geschädigten Person betroffen sein. Oft riskieren sie, dass ein E-Mail mit Malware oder Phishing an sie verschickt wird, welches scheinbar vom Konto des Kollegen oder Geschäftspartners kommt. Mit dieser Methode können die Angreifer weitere Zugänge im Firmennetzwerk gewinnen

Empfehlungen:

Technische Massnahmen:

- Nutzen Sie eine Zwei-Faktor-Authentifizierung wo immer diese verfügbar ist.
- Es wird empfohlen, einen Dienst zu wählen, der genügend Logging Funktionalität bietet und die Logs in geeigneter Form für Kunden zur Verfügung stellt.
- Den Unternehmen wird empfohlen, nach anormalen Aktionen bei den Konten der Mitarbeitenden zu suchen: Zugang von ungewöhnlichen Orten oder zu unüblichen Zeiten, Hinzufügen von E-Mail-Weiterleitungen, etc.
- Mails sollten (zumindest intern) immer digital signiert sein und Benutzer darauf trainiert werden, Mails ohne eine entsprechende Signatur besonders vorsichtig zu behandeln.
- Beim Versand von legitimen E-Mails mit hohem Missbrauchspotential für Phishing, wie z.B. der elektronische Versand von Rechnungen, sollte darauf geachtet werden, dass die Links nicht hinter HTML Text versteckt sind und dass die Mails und/oder Dokumente digital signiert sind.
- Damit die eigene Domain weniger einfach für Phishing Versuche missbraucht werden kann, sollte SPF, DKIM und DMARC Protokolle eingerichtet werden. Dies ist auch bei einigen der grossen Collaboration Providern möglich, wie z.B. bei Office365

Organisatorische Massnahmen:

- Die beste Methode, um Phishing zu bekämpfen, ist die Mitarbeitenden bezüglich diesem Phänomen zu sensibilisieren: Es ist unerlässlich, dass die Mitarbeitenden in der Erkennung und dem Umgang mit suspekten und betrügerischen E-Mails geschult werden. Sensibilisierte Mitarbeitende wissen, dass sie bei suspekten oder betrügerischen E-Mails auf keine Links klicken oder

Anhänge öffnen sollen, sondern umgehend die Vorgesetzten oder die IT-Verantwortlichen informieren sollten.

- Ebenfalls sind die vom Unternehmen definierten Prozesse und risikominimierenden Massnahmen zu jeder Zeit einzuhalten. Insbesondere sollten sämtliche Prozesse, welche den Zahlungsverkehr betreffen, firmenintern klar geregelt sein und von den Mitarbeitenden in allen Fällen eingehalten werden (z.B. Vier-Augen-Prinzip, Unterschrift kollektiv zu zweien, Prozesse gemäss internem Kontrollsystem).
- Die Phishing-Versuche können auf der Seite www.antiphishing.ch gemeldet werden. Dies erlaubt MELANI, schnelle Massnahmen zu treffen, um andere enutzer zu schützen.

✉ Fachkontakt

Letzte Änderung 02.10.2018

Merkblatt Informationssicherheit für KMUs

Phishing