Die neue Volkspartei

Presseunterlage zum Fälschungsskandal

Montag, 17. Juni 2019

Deloitte.

Deloitte Financial Advisory GmbH
Renngasse 1/ Freyung
Postfach 2
1010 Wien, Österreich

Tel +43 1 537 00 + DW
Fax +43 1 537 00-99 + DW
www.deloitte.at

www.deloitte.at

Stellungnahme

Datum:	16.06.2019
An:	Die neue Volkspartei („ÖVP“)
Von:	Deloitte Financial Advisory GmbH (“Deloitte”)
Betreff:	Korrespondenz Analyse („Projekt15“)

Gemäß Auftragsschreiben vom 15.06.2019 wurde die Analyse nachfolgend erhaltener „technische Hinweise" in Bezug auf eine gesendete E-Mail-Korrespondenz durchgeführt. Diese Informationen wurden uns am 15.06.2019 von Herrn Roman Kalinka (IT Abteilungsleiter ÖVP) zur Analyse zur Verfügung gestellt.

(version=TLS1 _2
cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128):

Thread-Index:
AQHUpk7smxGryDPJUE202WWP9+eAMK
Wk8MVg

Spf=neutral 92.51.182.1
Domain of
gernot.bluemel@wien.oevp.at

smtp.mailfrom=gernot.bluemel@wien.oevp.at

for

sebastian.kurz@wien.oevp.at

Mon, 27 Feb 2018 11.04:05
-800 (PST)

Received-SPF

Anhand dieser erhaltenen Teilinformationen einer potentiellen E-Mail-Korrespondenz ließen sich folgende Punkte feststellen. Es sei anzumerken, dass die oben angeführten „technischen Hinweise" nicht die vollständigen Metadaten eines E-Mail-Headers darstellen, sondern nur Teile davon in abgeänderter Reihenfolge abbilden (beispielsweise erscheint hier sehr untypisch das Feld „Received-SPF" am Ende und damit nach der eigentlichen SPF Information).

1. Das enthaltene **Datum** der E-Mail-Korrespondenz bezieht sich auf „**Mon, 27 Feb 2018 11.04:05**". Dabei ließen sich folgende Auffälligkeiten feststellen:
   - Der Wochentag Montag ist falsch gewählt da es sich beim 27.02.2018 um einen Dienstag handelte.
   - Das Format des Datums enthält einen Punkt („.") anstelle eines Doppelpunkts („:") zwischen Stunde und Minute.
   - Die nächste Zeile **PST** bezieht sich auf „Pacific Standard Time", einer Zeitzone die in Nord-Amerika verwendet wird.

   Datumsformate die von Servern oder IT-Systemen generiert und ausgegeben werden sind typischerweise konsistent und enthalten keine derartigen Fehler.

2. Der **Thread-Index** gibt Aufschlüsse über die Sendezeitpunkte einer oder mehrerer gesendeter E-Mail-Nachrichten innerhalb eines E-Mail-Threads (einer zusammenhängenden „Kette" an E-Mail-Nachrichten). Diese Information wird kodiert mit einer E-Mail-Nachricht übertragen und enthält neben dem Datum der einzelnen Nachrichten noch eine eindeutige ID pro E-Mail-Thread. Damit lassen sich nicht nur Beziehungen zwischen E-Mail-Nachrichten, sondern auch die Zeitpunkte und Zeitdifferenzen der E-Mail-Nachrichten eruieren.
   Die Rückrechnung[1] des angegebenen Thread-Index (**AQHUpk7smxGryDPJUE202WWP9+eAMKWk8MVg**) zeigte, dass es sich um zwei E-Mail-Nachrichten handelt. Demnach eine E-Mail und eine dazugehörige Antwort- oder Weiterleitungs-E-Mail. Jedoch resultierte die Rückrechnung des Thread-Index nur in folgenden beiden (fehlerhaften) Sendezeitpunkten:
   - 1830-12-23 09:19:36.838758
   - 1833-04-14 13:45:09.903564

   Dieser Datumsbereich ist nicht schlüssig. Die generelle Rückrechnung des Thread-Index konnte mit aktuellen E-Mail-Nachrichten erfolgreich nachgestellt werden. Als Grund für diesen konkreten falschen Datumsbereich können damalige technische Probleme nicht ausgeschlossen werden.

3. Das angegebene **TLS Verschlüsselungsprotokoll** konnte aufgrund der zeitlichen Differenz nicht mit den damaligen Konfigurationen der ÖVP Mailserver abgeglichen

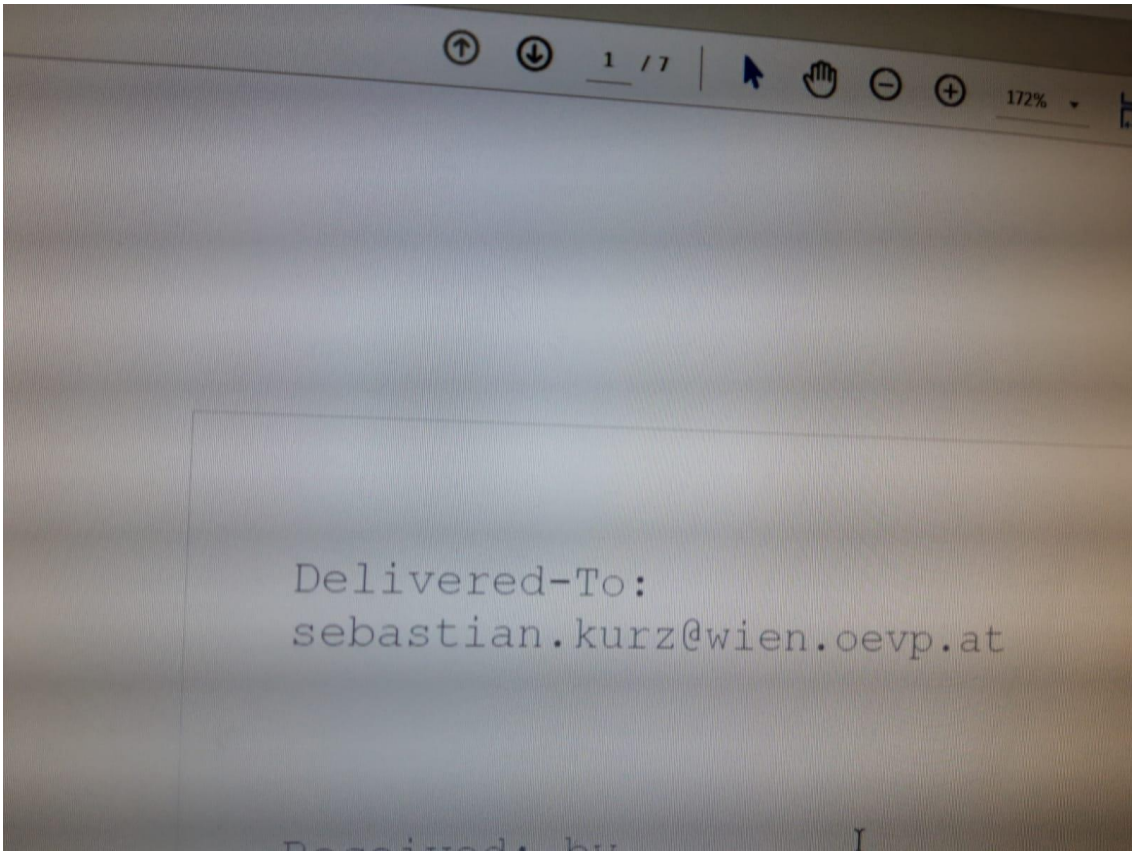
[1] Microsoft PidTagConversationIndex:
https://docs.microsoft.com/en-us/openspecs/exchange_server_protocols/ms-oxomsg/9e994fbb-b839-495f-84e3-2c8c02c7dd9b
Rückrechnung erfolgte mittels zwei separater Tools, von:
https://stackoverflow.com/questions/27374077/parsing-thread-index-mail-header-with-python
https://technical.nttsecurity.com/post/102enx6/outlook-thread-index-value-analysis

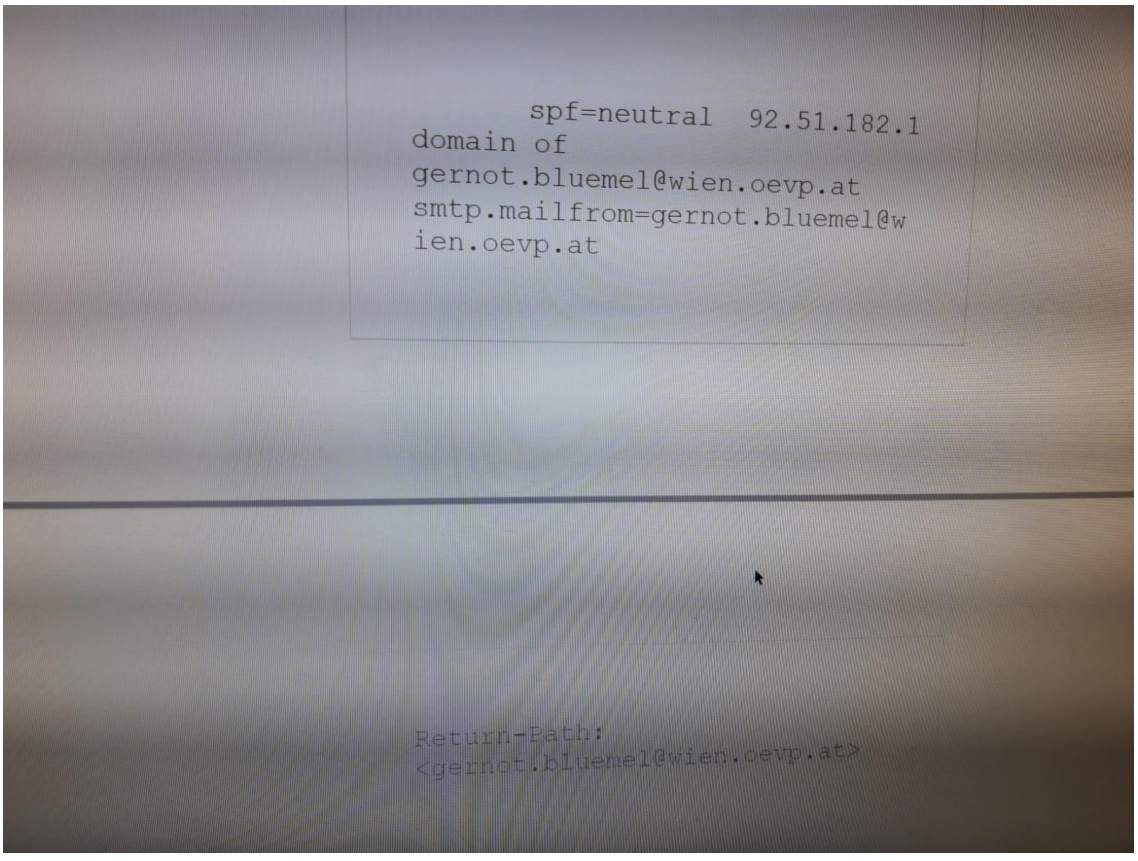
werden. Laut Auskunft durch Herrn Roman Kalinka wird das Protokoll **TLS1.2** jedoch erst seit Anfang 2019 unterstützt und war zum damaligen Zeitpunkt 2018 in deren Infrastruktur noch nicht aktiv.
Weiters ist anzumerken, dass aufgrund einer Serverkonfiguration zum gegebenen Zeitpunkt ein Versand von der Mailadresse sebastian.kurz@wien.oevp.at, laut Auskunft von Herrn Roman Kalinka (IT Abteilungsleiter ÖVP), nicht möglich war.

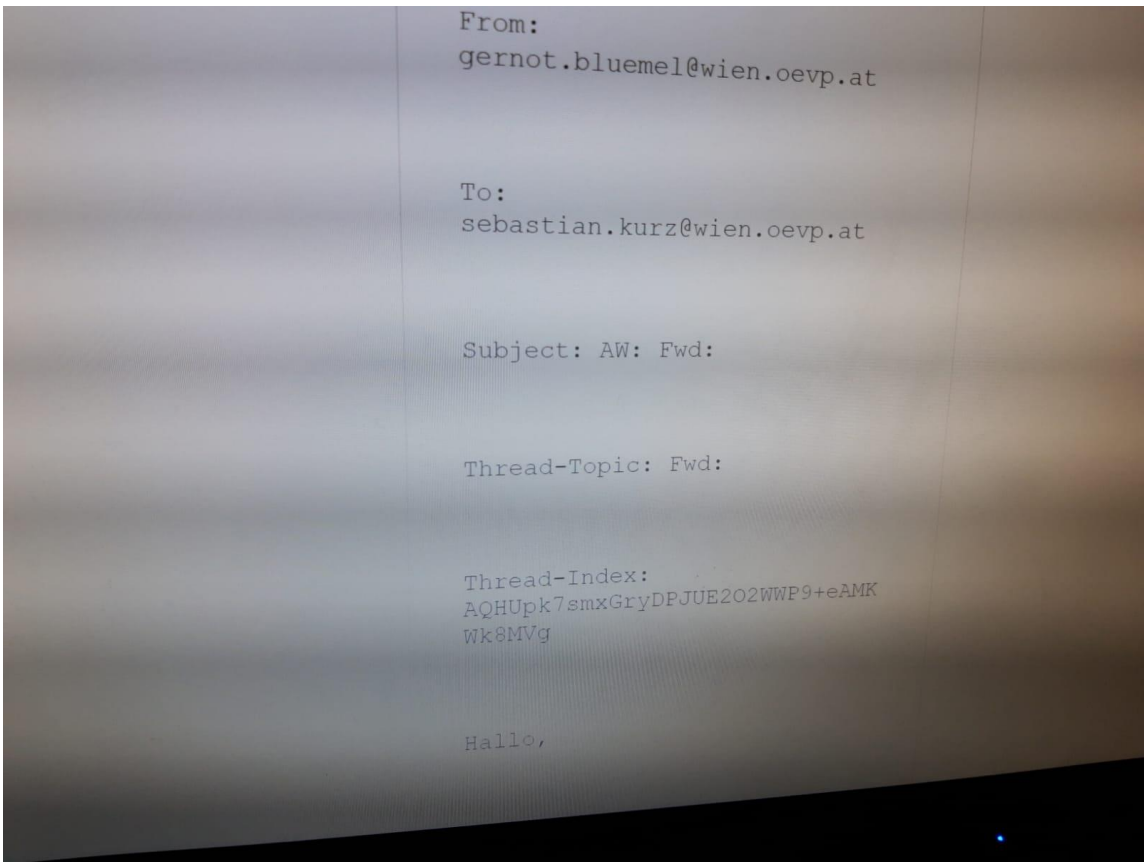
4. **SPF (Sender Policy Framework)** ist ein Verfahren um die Absenderadresse einer E-Mail-Korrespondenz zu überprüfen. Es wird in der entsprechenden DNS Zone (Domain Name System Zone) ein Eintrag hinterlegt, der angibt welche IP-Adressen und damit welche Mailserver für die entsprechende Domäne E-Mails versenden dürfen.
   Die hier erhaltene IP Adresse (**92.51.182.1**) ist derzeit auf „hosteurope.de" registriert und nicht auf wien.oevp.at, wie bei einer internen Kommunikation (innerhalb der wien.oevp.at Domäne) anzunehmen wäre. Weiters wäre eine SPF Überprüfung bei einer rein internen Kommunikation innerhalb der Domäne (wien.oevp.at) grundsätzlich nicht notwendig, hängt jedoch von der damaligen Systemkonfiguration ab. Eine zum jetzigen Zeitpunkt durchgeführte SPF Abfrage der Domäne wien.oevp.at sowie oevp.at von dem entsprechenden DNS-Server zeigt diesen IP-Eintrag (92.51.182.1) nicht an. Das SPF Ergebnis „neutral" [2] deutet weiters darauf hin, dass die SPF-Absenderüberprüfung zum damaligen Zeitpunkt kein Ergebnis zu dem Absender lieferte (weder SPF „pass" noch „fail").

[2] https://tools.ietf.org/html/rfc7208#section-2.6

Screenshots






From:
gernot.bluemel@wien.oevp.at

To:
sebastian.kurz@wien.oevp.at

Subject: AW: Fwd:

Thread-Topic: Fwd:

Thread-Index:
AQHUpk7smxGryDPJUE2O2WWP9+eAMK
Wk8MVg

Hallo,