Assignment #4: Messagedetails

Lecture: D3.2: Information Security and Privacy
Abgabe: 18.11.2022 - 12:00 - per Moodle

1. Die letzte Vorlesung thematisierte einen Phishingversuch auf die User der Rheinischen Post. User der Kunstakademie Düsseldorf sind Opfer einen Spammail geworden, welche es auch auf Phishing abgesehen hatte. Die User wenden sich an Sie, Sie sind Teil der lokalen IT Abteilung, um zu erfahren, wie verfahren werden soll und woher der Angriff überhaupt kommt.

   Untersuchen Sie die folgenden Nachrichtendetails (auffindbar auf der letzten Seite des Dokumentes) auf markante Punkte, die Ihnen verraten, woher die Mail stammen könnte. Tipp: Sie findend die Nachrichtendetails im Kursordner als .txt Datei, die durchsuchbar ist.

   (a) (4p.) Geben Sie in Stichpunkten an, woher die Mail stammen könnte, geben Sie dabei die Quelle Ihrer Vermutung mit der Zeilennummer an.

   (b) (4p.) Welchen Dienst, welchen Anbieters, nutzt die Kunstakademie Düsseldorf um sich vor Phishingversuchen Dritter zu schützen. Begründen Sie Ihre Antwort mit einer Referenz auf die jeweilige Zeilennummer.

   (c) (2p.) Nennen Sie in kurzen Stichpunkten (2-3 Stichpunkte) wie Sie gegen solch eine Phishing Mail vorgehen würden.

```
Received: from kadWEBMAIL1.kad.de (10.111.244.22) by
 kadWEBMAIL1.kad.de (10.111.244.22) with Microsoft SMTP Server
 (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.2.986.5
 via Mailbox Transport; Sat, 12 Feb 2022 17:01:28 +0100
Received: from kadWEBMAIL1.kad.de (10.111.244.22) by
 kadWEBMAIL1.kad.de (10.111.244.22) with Microsoft SMTP Server
 (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.2.986.5;
 Sat, 12 Feb 2022 17:01:28 +0100
Received: from b2481.mx.srv.dfn.de (10.111.244.31) by kadWEBMAIL1.kad.de
 (10.111.244.22) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.2.986.5 via Frontend
 Transport; Sat, 12 Feb 2022 17:01:28 +0100
Received: from localhost (localhost [127.0.0.1])
    by b2481.mx.srv.dfn.de (Postfix) with ESMTP id 7D6F320086
    for <joerg.cosfeld@kad.de>; Sat, 12 Feb 2022 17:01:28 +0100 (CET)
X-Virus-Scanned: Debian amavisd-new at mgw5-tub.srv.dfn.de
X-Spam-Flag: YES
X-Spam-Score: 7.758
X-Spam-Level: *******
X-Spam-Status: Yes, score=7.758 tagged_above=2 required=6.2 tests=[BAYES_80=4,
    BOGO_SPAM=3, HTML_FONT_LOW_CONTRAST=0.001, HTML_MESSAGE=0.001,
    MIME_HTML_ONLY=0.1, RCVD_IN_MSPIKE_BL=0.001, RCVD_IN_MSPIKE_L4=0.001,
    SPF_HELO_PASS=-0.001, SPF_SOFTFAIL=0.665, T_SCC_BODY_TEXT_LINE=-0.01]
    autolearn=disabled
Received: from b2481.mx.srv.dfn.de ([127.0.0.1])
    by localhost (mgw5-tub.srv.dfn.de [127.0.0.1]) (amavisd-new, port 20178)
    with ESMTP id LR9awu-MT0Ns
    for <joerg.cosfeld@kad.de>;
    Sat, 12 Feb 2022 17:01:27 +0100 (CET)
Received: from atl4mhho05.registeredsite.com (atl4mhho05.registeredsite.com
    [209.17.115.113])
    by b2481.mx.srv.dfn.de (Postfix) with ESMTPS
    for <joerg.cosfeld@kad.de>; Sat, 12 Feb 2022 17:01:26 +0100 (CET)
Received: from atl4wpplatweb12b.registeredsite.com ([10.30.52.29])
    by atl4mhho05.registeredsite.com (8.14.4/8.14.4) with ESMTP id 21
    CG1IJM034304
    (version=TLSv1/SSLv3 cipher=DHE-RSA-AES256-GCM-SHA384 bits=256 verify=NO)
    for <joerg.cosfeld@kad.de>; Sat, 12 Feb 2022 11:01:18 -0500
Received: from atl4wpplatweb12b.registeredsite.com (localhost [127.0.0.1])
    by atl4wpplatweb12b.registeredsite.com (8.14.7/8.14.4) with ESMTP id 21
    CG1IUf004172
    for <joerg.cosfeld@kad.de>; Sat, 12 Feb 2022 11:01:18 -0500
Received: (from 8aa7c17161d6a6270218e8a7b0806263@localhost)
    by atl4wpplatweb12b.registeredsite.com (8.14.7/8.14.7/Submit) id 21
    CG1I34004171;
    Sat, 12 Feb 2022 11:01:18 -0500
X-Authentication-Warning: atl4wpplatweb12b.registeredsite.com: 8
    aa7c17161d6a6270218e8a7b0806263 set sender to joerg.cosfeld@kad.de using -
    f
To: <joerg.cosfeld@kad.de>
Subject: FDW : verzend uw pakket DE- 97619319913077
Date: Sat, 12 Feb 2022 11:01:18 -0500
From: Support <joerg.cosfeld@kad.de>
Message-ID: <Pmcv5VBqZfGMWHoeKHF2CYwdhtxTtRePbeI7QXEQ@venessariley.05a055f.
    netsolhost.com>
X-Mailer: PHPMailer 6.0.7
```

```
MIME-Version: 1.0
Content-Type: text/html; charset="UTF-8"
Content-Transfer-Encoding: 8bit
Return-Path: joerg.cosfeld@kad.de
X-MS-Exchange-Organization-Network-Message-Id: c35544f8-cbf2-4c78-6a99-08
    d9ee40eded
X-MS-Exchange-Organization-PRD: kad.de
X-MS-Exchange-Organization-SenderIdResult: SoftFail
Received-SPF: SoftFail (kadWEBMAIL1.kad.de: domain of transitioning
 joerg.cosfeld@kad.de discourages use of 10.111.244.31 as
 permitted sender)
X-MS-Exchange-Organization-SCL: 0
X-MS-Exchange-Organization-PCL: 2
X-MS-Exchange-Organization-Antispam-Report: DV:3.3.5705.600;SID:SenderIDStatus
 SoftFail;OrigIP:10.111.244.31
X-MS-Exchange-Organization-AuthSource: kadWEBMAIL1.kad.de
X-MS-Exchange-Organization-AuthAs: Anonymous
X-MS-Exchange-Transport-EndToEndLatency: 00:00:00.2804662
X-MS-Exchange-Processed-By-BccFoldering: 15.02.0986.005
```

Listing 1: message details