Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD
Generalsekretariat

Nationales Zentrum für Cybersicherheit NCSC
www.ncsc.admin.ch

NCSC

Home Office:

Endbenutzer Guideline

Einleitung

Als Ergänzung zum Dokument “Home-Office: Sicherer Umgang mit Fernzugriffen” möchten wir eine kurze Information für den Endbenutzer bereitstellen, wie er seine eigene Umgebung besser schützen kann und somit auch das Risiko für den Arbeitgeber zu reduzieren vermag.

Empfehlungen

Zugang zum System

- Der Zugriff auf Ihren Computer muss in jedem Fall mit einem **starken Passwort** geschützt sein. Falls Ihre Firma eine **2 Faktor Authentisierung** für Firmengeräte verwendet, lassen Sie die Smartcard/Dongle nicht stecken, wenn Sie die Wohnung verlassen, sondern bewahren Sie diese separat auf.
- Arbeiten Sie mit einem **BYOD** („Bring Your Own Device“, eigenes, nicht vom Arbeitgeber gestelltes) Gerät, passen Sie die Sicherheitseinstellungen sinngemäss an. Fragen Sie im Zweifelsfalle ihre IT-Abteilung nach einer kurzen Anleitung.
- Verwenden Sie einen **Bildschirmschoner** mit **Passwort**, der sich nach spätestens 15min Inaktivität aktiviert.
- Verwenden Sie einen **Passwortmanager** für das Speichern Ihrer Passwörter. Entweder die Lösung, die Ihnen Ihr Arbeitgeber zur Verfügung stellt, oder (am besten) einen Offline Passwort Manager wie z.B. KeePass (https://keepass.info/)
- Prüfen Sie, ob die **Datenträgerverschlüsselung** auf Ihrem Arbeitsplatzrechner aktiv ist. Wenn Sie sich nicht sicher sind, fragen Sie Ihre IT-Abteilung.
- Wenn Sie Ihren Arbeitscomputer mit Ihrem **Heimnetzwerk** verbinden, stellen Sie sicher, dass Sie ihn nicht für andere Computer im Netzwerk sichtbar machen. Wenn Sie ihn der Heimnetzgruppe hinzufügen müssen, stellen Sie sicher, dass die Option zum Freigeben von Dateien ausgeschaltet ist.

Sichere Verbindungen

- Stellen Sie sicher, dass Sie Zugriff auf die Infrastruktur Ihres Unternehmens haben und sich über das **VPN/ den Remote Zugang** Ihrer Firma einwählen können.
- **Sichern** Sie Ihr **Wi-Fi** zu Hause mit einem starken Kennwort, verwenden Sie immer WPA2 oder falls auf Ihrem Gerät schon verfügbar WPA3.
- Der Zugriff auf die Einstellungen Ihres Heim-Routers sollte ebenfalls durch ein Kennwort geschützt sein. Achten Sie darauf, das Standardkennwort zu ändern. Informationen, wie Sie das tun können, sollten Sie im Internet auf der Herstellerwebseite Ihres Router Modells finden.

- Achten Sie darauf, dass Ihr Heimrouter immer eine **aktuelle Version der Software** hat.
- Falls Ihr normaler Internet Traffic nicht durch das Firmennetzwerk geschickt wird, haben Sie weniger Schutz. Seien Sie entsprechend vorsichtiger beim Surfen / Mailen. Falls Ihr gesamter Traffic durch das Firmennetzwerk geht (via ein VPN), sollten Sie sparsam mit der Bandbreite umgehen und z.B. auf YouTube/Streaming auf diesem Gerät verzichten.

Datensicherheit

- Verwenden Sie **keine private Cloud Datenspeicher** für geschäftliche Dokumente
- Vermischen Sie private und geschäftliche Daten nicht. Arbeiten Sie mit einem eigenen Gerät, erstellen Sie einen verschlüsselten Container für die geschäftlichen Daten, z.B. indem Sie einen USB Stick verschlüsseln oder verschlüsseln Sie die gesamte Festplatte mit Bitlocker[1].
- Achten Sie darauf, dass Sie lokal gespeicherte Daten mit einem **Backup** sichern. Verwenden Sie zwei unterschiedliche Disks oder USB Sticks und bewahren Sie diese sicher auf. Achten Sie darauf, dass ein Medium nicht am Computer angeschlossen bleibt, sondern immer nach Abschluss des Backups wieder ausgeworfen wird.

Physische Sicherheit im Home Office

- Wenn Sie Ihre Wohnung verlassen müssen, stellen Sie sicher, dass Ihre Arbeitsgeräte entweder ausgeschaltet oder gesperrt sind - einschliesslich aller Mobiltelefone, die Sie zum Abrufen von E-Mails oder zum Telefonieren auf der Arbeit benutzen könnten.
- Wenn Sie in einem **Mehrpersonenhaushalt** leben, insbesondere mit kleinen Kindern leben, sollten Sie Ihren Computer auch dann sperren, wenn Sie nur kurz vom Arbeitsplatz weggehen, um unabsichtlichen Manipulationen vorzubeugen.
- Wenn Sie keinen separaten **Arbeitsplatz** in Ihrer Wohnung einrichten können, sollten Sie Ihre Geräte am Ende Ihres Arbeitstages an einem sicheren Ort aufbewahren, an dem sie nicht mehr sichtbar sind. Dadurch wird nicht nur verhindert, dass sie versehentlich geöffnet oder gestohlen werden, sondern erleichtert auch die Trennung zwischen Ihrem Arbeitsleben und Ihrem Privatleben.

[1] https://www.heise.de/tipps-tricks/BitLocker-auf-Windows-10-Festplatte-richtig-verschluesseln-4325375.html#%C3%9Cberschrift_3
https://www.windowscentral.com/how-use-bitlocker-encryption-windows-10 (in englisch)

Trennen Sie Arbeitsgeräte und persönliche Geräte

- Bezahlen Sie Ihre Rechnungen zu Hause nicht auf demselben Computer, auf dem Sie arbeiten. Sie können nicht nur Verwirrung für sich selbst stiften, sondern auch Ihre persönlichen Daten kompromittieren, wenn ein Cyberkrimineller versucht hat, in Ihr Unternehmen einzudringen.
- Senden Sie keine arbeitsbezogenen E-Mails von Ihrer privaten E-Mail-Adresse aus und umgekehrt.
- Apropos **Heimunterricht**: Es ist wichtig, den digitalen Lehrplan Ihres Kindes von Ihrem Arbeitsgerät getrennt zu halten.
- Lassen Sie niemanden in Ihrem Haushalt auf Ihren Arbeitsrechner zugreifen, auch nicht, wenn Sie danebensitzen.

Allgemeine Cybersicherheit

- Wenn Sie **Programme** oder **Software** aus dem **Internet** herunterladen müssen, verifizieren Sie, dass Sie sich wirklich auf der Herstellerwebseite befinden und keine Schadsoftware herunterladen (Angreifer geben sich gerne als bekannte Firmen und Behörden aus[1]). Vor allem, wenn Sie Kollaborationssoftware im Zuge von Home Office herunterladen (z.B. Konferenzsoftware).
- **Phishing-E-Mails**: Viele Angreifer versuchen, aus der Aktualität und die Aufmerksamkeit, die diese generieren kann, Kapital zu schlagen (ein typisches Beispiel hierzu ist die Corona / Covid-19 Krise), und behaupten Information zu haben, Ratschläge zu erteilen oder Fragen zu diesem Thema zu stellen. Prüfen Sie solche E-Mails mit einem scharfen Auge und öffnen Sie keine Anhänge, es sei denn, sie stammen von einer Ihnen bekannten, vertrauenswürdigen Quelle. Achten Sie besonders auf diejenigen E-Mails, die sich als hochrangige Mitarbeiter tarnen, und achten Sie genau auf die tatsächliche E-Mail-Adresse des Absenders. Beachten Sie, dass die Absender-Adresse gefälscht sein kann und die richtige Absender-Adresse nur in den E-Mail-Kopfzeilen (E-Mail Header) ersichtlich ist.[2]
- Fragen Sie im Zweifelsfall immer beim Absender direkt nach (idealerweise telefonisch)
- Melden Sie sich im Zweifelsfall bei Ihrem Helpdesk / Ihrer IT-Abteilung
- Phishing E-Mails oder E-Mails mit Attachments können Sie auf https://www.antiphishing.ch melden. Beachten Sie bitte, dass diese Meldungen

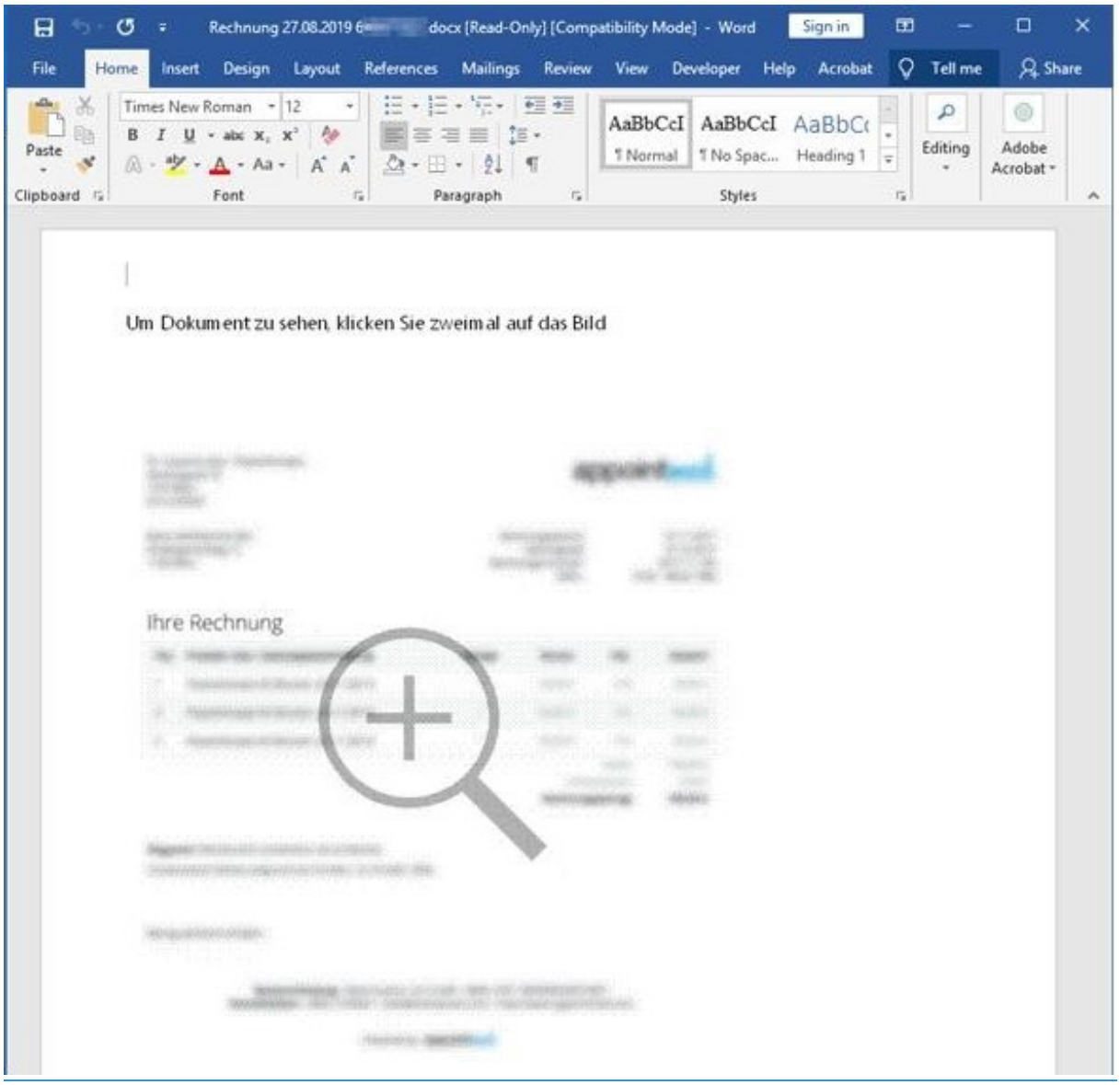
---

1 https://www.ncsc.admin.ch/ncsc/de/home/aktuell/news/news-archiv/zunehmender-missbrauch-der-namen-von-bundesstellen-und-firmen.html

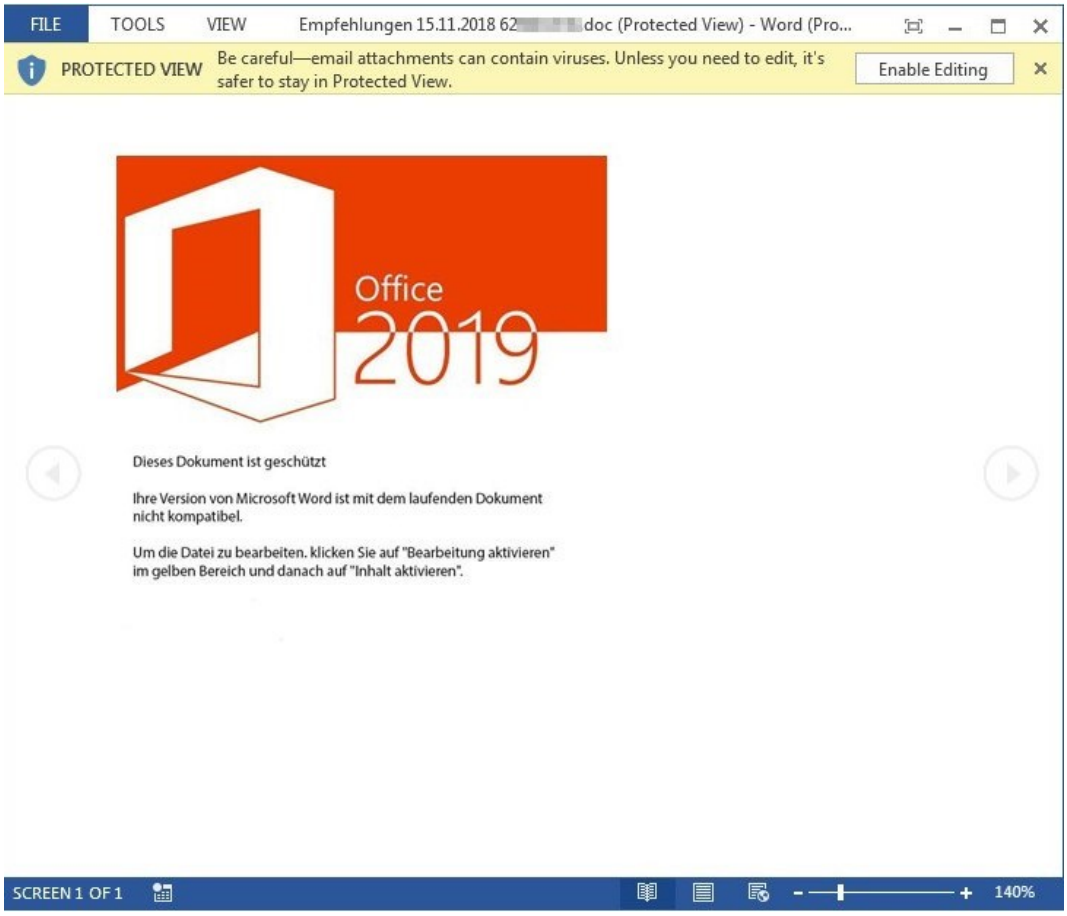
2 http://www.was-ist-malware.de/it-sicherheit/mail-spoofing/ und https://www.howtogeek.com/121532/htg-explains-how-scammers-forge-email-addresses-and-how-you-can-tell/ (in englisch)

automatisiert verarbeitet werden und Sie keine Rückmeldung erhalten. Falls Sie einen Fall melden möchten und eine Rückmeldung benötigen, kontaktieren Sie die Nationale Anlaufstelle via Meldeformular (https://www.report.ncsc.admin.ch/de/).

- **Aktivieren** Sie **keinesfalls Makros** und ignorieren Sie nie Sicherheitswarnungen, wenn Sie ein Dokument öffnen, welches über E-Mail versendet worden ist oder das Sie vom Internet heruntergeladen haben. Öffnen Sie im Zweifelsfall das Dokument lieber nicht und fragen Sie beim Absender telefonisch nach oder melden Sie sich bei Ihrer IT-Abteilung. Nachfolgend sehen Sie auf Screenshot 1 und 2 Beispiele von Word-Anhängen mit Makros.



Screenshot 1: Durch das Doppelklicken auf das Bild werden Makros ausgeführt, und Ihr PC wird Schadsoftware infiziert.



Screenshot 2: Durch das Drücken von «Enable Editing» oder «Bearbeiten aktivieren» werden die Makros ausgeführt, und sie werden mit Schadsoftware infiziert.

Bei Fragen zu diesem Dokument kontaktieren Sie bitte outreach[at]ncsc.ch.