ARBEITSANWEISUNG FÜR ANGESTELLTE MIT BETRIEBSGERÄTEN

ISTRUZIONI DI LAVORO PER DIPENDENTI CON DISPOSITIVI AZIENDALI

Diese Arbeitsanweisung soll dazu beitragen, dass die Rechtsvorschriften zur Verarbeitung personenbezogener Daten und zum Schutz der informationstechnischen Systeme eingehalten werden und insbesondere die Vertraulichkeit, Integrität und Verfügbarkeit von betrieblichen/geschäftlichen Dokumenten und Informationen sowie damit zusammenhängenden personenbezogenen Daten gewährleistet werden kann, sowohl am Arbeitsplatz im Büro als auch im Homeoffice.

Le presenti istruzioni di lavoro hanno lo scopo di contribuire a garantire il rispetto delle disposizioni di legge sul trattamento dei dati personali e della sicurezza informatica e, in particolare, che possa essere garantita la riservatezza, l'integrità e la disponibilità di documenti e informazioni aziendali/d'ufficio e dei collegati dati personali, sia sul posto di lavoro in ufficio, sia in sede di telelavoro.

Anwendbare Normen: Verordnung (EU) 2016/679, Art. 32, sowie Vorgaben der Autorità Garante per la protezione dei dati personali

Präventionsrichtlinien der ENISA

Präventionsrichtlinien von EUROPOL

Norme applicabili: Regolamento (UE) 2016/679, Art. 32, nonché specifiche dell'Autorità Garante per la protezione dei dati personali

Linee guida ENISA

Linee guida EUROPOL

1. VORGABEN BETRIEBSGERÄTE

UPDATES

1.1. Der Arbeitgeber/Verantwortliche stattet die Betriebsgeräte mit den nötigen Sicherheitsvorkehrungen aus (PC's und Laptops z.B. mit Antivirus; Tablets und Smartphones mit MDM-Software). Die Betriebssysteme und Programme auf PCs, Smartphones und Tablets sind immer auf dem aktuellen Stand zu halten. Mit Updates werden meist Sicherheitsschwachstellen behoben.

PASSWÖRTER

1.2. Starke Passwörter schützen Systeme und Daten vor dem Zugriff durch Unberechtigte. Die Passwörter müssen den gängigen Sicherheitsstandards des Arbeitgebers/Verantwortlichen entsprechen.

VERBINDUNG

1.3. Der Zugriff auf Daten des Arbeitgebers/Verantwortlichen darf – abgesehen klarerweise von all jenen Fällen, in denen das

1. DIRETTIVE PER L'UTILIZZO DI DISPOSITIVI AZIENDALI

UPDATES

1.1. Il datore di lavoro/Titolare equipaggia i dispositivi aziendali con le necessarie misure di sicurezza (PC e laptop, p.es., con antivirus; tablet e smartphone con software MDM). I sistemi operativi e i programmi su PC, smartphone e tablet devono essere sempre tenuti aggiornati.

Gli aggiornamenti vengono solitamente utilizzati per correggere le vulnerabilità della sicurezza.

PASSWORD

1.2. Password complesse proteggono sistemi e dati da accessi non autorizzati. Le password devono corrispondere alle prescrizioni del datore di lavoro/Titolare di trattamento.

CONNESSIONE

1.3. È possibile accedere ai dati del datore di

lavoro/Titolare di trattamento – e fatti comunque

Betriebsgerät direkt (z.B. mittels Ethernet-Kabel) am Netz des Arbeitsgebers angeschlossen wird – ausschließlich über eine sichere, vom Arbeitgeber bereitgestellte, VPN-Verbindung/ Remote Desktop erfolgen; davon abgesehen ist der Zugang mittels der betrieblich zugelassenen Cloud-Lösungen/ webbasierten Anwendungen erlaubt (vgl. hierzu die eigenen "Verwendungsvorgaben für die Angestellten in Bezug auf Cloud-Lösungen"). Die Zugangsdaten werden Ihnen vorab mitgeteilt.

Es ist keine Verwendung von VPN- oder anderen – z.B. Tor – ähnlichen Diensten zur Verschleierung des Standortes, ob beabsichtigt oder nicht, zulässig.

SICHERE IDENTIFIKATION

1.4. Die im vorhergehenden Punkt beschriebenen Zugriffe sind als streng persönlich einzustufen und die entsprechenden Passwörter dürfen niemals an Dritte weitergegeben werden.

salvi tutti i casi in cui il dispositivo aziendale venga collegato direttamente alla rete del datore di lavoro (p.es. Tramite cavo Ethernet) – solo tramite una connessione VPN sicura/Remote Desktop messa a disposizione dal datore di lavoro; oltre a ciò, è ammesso l'accesso tramite soluzioni Cloud/applicazioni basate sul web autorizzate dall'azienda (cfr. in merito le specifiche "Linee guida per dipendenti per l'utilizzo di soluzioni Cloud"). Le verranno fornite le credenziali di accesso in anticipo.

Non è ammesso l'utilizzo, intenzionale o meno, di VPN- o altri servizi (p.es. Tor) funzionali ad occultare la localizzazione.

IDENTIFICAZIONE SICURA

1.4. Gli accessi descritti al punto precedente sono da intendersi come strettamente personali e le relative password non devono mai essere comunicate a terzi.

2. WEITERE VORGABEN

2. ALTRE PRESCRIZIONI

GESCHÄFTLICHE DOKUMENTE, INFORMATIONEN UND PERSONENBEZOGENE DATEN SCHÜTZEN

2.1. Dokumente, Informationen und personenbezogene Daten sind zu schützen, auch im Homeoffice:

- die Inhalte des/r vom Arbeitgeber/Verantwortlichen erteilten Auftrags und Anweisungen gemäß Art. 29 EU-Verordnung Nr. 679/2016 für die Verarbeitung von personenbezogenen Daten sind auch im Zuge der Verwendung von Betriebsgeräten einzuhalten;

- Zugangspasswörter sind geheim zu halten;

- Interne informationen und personenbezogene Daten sind vor Unberechtigten, auch Familienmitgliedern, zu schützen;

- Der Bildschirm ist vor Einsicht zu schützen;

-Auf dem Betriebsgerät sind keine personenbezogenen Daten privater Natur zu speichern;

- Papierdossiers und Ausdrucke sind vor

PROTEGGERE I DATI PERSONALI E SEGRETI D'UFFICIO (DOCUMENTI, INFORMAZIONI)

2.1. Documenti, informazioni e dati personali devono essere protetti, anche durante il telelavoro:

- I contenuti dell'incarico e delle istruzioni del datore di lavoro/Titolare di trattamento ex art. 29 regolamento UE n. 679/2016 per il trattamento dei dati personali sono da rispettare anche nell'utilizzo dei dispositivi aziendali;

- Le password di accesso devono essere tenute segrete;

- Le informazioni interne e i dati personali devono essere protetti da persone non autorizzate, compresi i familiari;

- Lo schermo deve essere protetto dalla vista di terzi,

- Sul dispositivo aziendale non devono essere salvati dati di natura privata;

- I fascicoli cartacei e le stampe devono essere protetti dall'accesso non autorizzato;

unberechtigtem Zugriff zu schützen;

- Nicht mehr benötigte Papierunterlagen sind zu schreddern oder sicher aufzubewahren, bis sie im Büro vernichtet werden können.

- I documenti cartacei non più necessari devono essere distrutti o conservati in un luogo sicuro fino a quando non possono essere distrutti in ufficio.

E-MAIL SICHER EINSETZEN

2.2. Die Nutzung privater E-Mail-Konten für die geschäftliche Kommunikation ist verboten. Geschäftliche E-Mails dürfen nicht auf private Konten weitergeleitet werden.

UTILIZZO SICURO DELLE MAIL

2.2. È vietato utilizzare account di posta elettronica privati per la comunicazione aziendale. Le e-mail aziendali non devono essere inoltrate ad account personali.

KOMMUNIKATIONS-TOOLS GEZIELT AUSWÄHLEN

2.3. Neben dem Telefon und den E-Mails werden auch Messengers und Videokonferenzdienste eingesetzt. Informationen zu den Diensten erhalten Sie auf Anfrage beim IT-Verantwortlichen.

SELEZIONE MIRATA DEGLI STRUMENTI DI COMUNICAZIONE

2.3. Oltre al telefono e alla posta elettronica, vengono utilizzati anche servizi di messaggistica e videoconferenza. Le informazioni sui servizi sono disponibili su richiesta presso il responsabile del reparto informatico.

SICH VOR PHISHING UND ANDEREN BEDROHUNGEN SCHÜTZEN

2.4. Verdächtige E-Mails dürfen nicht geöffnet werden. Anhänge in Mails von unbekannten Absendern dürfen nicht angeklickt werden. Im Zweifel ist die Absenderin oder der Absender per Telefon zu kontaktieren, damit sie oder er den Inhalt der E-Mail bestätigen kann.

PROTEGGETEVI DAL PHISHING E DA ALTRE MINACCE

2.4. Le e-mail sospette non devono essere aperte. Non fare clic sugli allegati nelle e-mail di mittenti sconosciuti. In caso di dubbio, il mittente deve essere contattato telefonicamente in modo che possa confermare il contenuto dell'e-mail.

DATENSCHUTZVERLETZUNGEN SOFORT MELDEN

2.5. Wenn Arbeitsmittel wie Dokumente oder auch Ihr PC verloren gehen oder abhandenkommen, ist dies umgehend dem Vorgesetzten zu melden.

SEGNALARE IMMEDIATAMENTE I DATA BREACH

2.5. In caso di smarrimento di documenti o apparecchiature di lavoro è necessario segnalarlo immediatamente al responsabile di reparto.

Zusätzliche Informationen zum Thema IT-Sicherheit im Privathaushalt finden Sie unter: https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/make-your-home-cyber-safe-stronghold

Altre informazioni riguardanti la sicurezza informatica a casa Vostra trovate sotto: https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/make-your-home-cyber-safe-stronghold

3. KONTROLLEN

3. VERIFICHE

3.1. Die Tätigkeiten der Mitarbeiter mittels Betriebsgeräten werden nicht systematisch und kontinuierlich überwacht, die Systemadministratoren des Arbeitgebers/Verantwortlichen (auch in Zusammenarbeit mit der EDV-Abteilung) können die Nutzung (= die Tätigkeiten auf den Servern des Arbeitgebers/Verantwortlichen, so z.B. die erzeugten Logfiles; bei Bedarf auch direkte

3.1 Le attività dei dipendenti svolte tramite dispositivi aziendali non sono soggetti a una sorveglianza sistematica e continua, ma gli amministratori di sistema del datore di lavoro/Titolare (anche in collaborazione con la Ripartizione CED) possono monitorare o indagare sull'utilizzo (= le attività sui server del datore di lavoro/Titolare, così p.es. i logfiles generati; al bisogno anche verifica diretta del dispositivo

Überprüfung des Betriebsgerätes selbst; usw.) aber überwachen oder untersuchen; dies geschieht nur, um die Einhaltung der relevanten Richtlinien zu bestätigen und mögliche Sicherheitsverletzungen, unbefugte Zugriffe, technische Probleme, usw. zu untersuchen und nicht für die Zwecke der Überwachung der Arbeitstätigkeit. Die Verwendung von Logfiles erfolgt immer mit einer festgelegten zeitlichen Begrenzung (kurze Frist) und Tracing-Tätigkeit erfolgt nur bei allfälligen Verdachtsmomenten, in manueller Form und üblicherweise in direkter Zusammenarbeit mit dem betroffenen Nutzer.

aziendale); ciò si verificherà solo per confermare la conformità ai requisiti della politica pertinente e per indagare su possibili violazioni della sicurezza, accessi non autorizzati, problemi tecnici, ecc. e non ai fini del monitoraggio dell'attività lavorativa. L'utilizzo di logfiles è limitato a tempistiche prefissate (breve termine) e l'attività di tracing viene espletata solo nei casi di dubbio, in forma manuale e di regola in collaborazione diretta con l'utente interessato.

Die Kontrollen können wie folgt zusammengefasst werden:

1) Kontrolle/Einschränkung auf der Grundlage der IP der Region, aus welcher der Verbindungszugriff erfolgt (ev. auch für weitere Dienste)
2) Kontrolle/Einschränkung auf der Grundlage der IP für den E-Mail-Zugang
3) Befähigung bestimmter IP's in Zusammenhang mit kritischen Diensten (z.B. Meldedaten an die Polizeikräfte)
4) zusätzliche Kontrollformen, die im Laufe der Zeit, zur best practice des Sektors zählen werden (z.B. conditional access und multifactor autentication, usw.)

Le attività di controllo possono essere così riassunte:

1) controllo/restrizione su base IP della regione di accesso per collegamento VPN (ev. anche per altri servizi)
2) controllo/restrizione su base IP per l'accesso alle e-mail
3) abilitazione su IP specifici dei servizi critici (es. anagrafe alle forze dell'ordine)
4) ulteriori forme di controllo che costituiranno, nel continuo, la best practice di settore (p.es. conditional access e multifactor autentication, ecc.)

4. RECHT AUF NICHTERREICHBARKEIT

Im Fall von Telearbeit/Smartworking sieht die individuelle Vereinbarung zwischen Arbeitgeber und Angestellten u.a. die Ruhepausen mit Anrecht auf Unterbrechung der Verbindung vor.

4. DIRITTO ALLA DISCONNESSIONE

In caso di telelavoro/smartworking l'accordo individuale tra il datore di lavoro e il dipendente prevede, tra l'altro, i tempi di riposo con diritto alla disconnessione;