ATIC · GIZ · DT4SME

AGENDA

Protejarea proceselor, datelor și infrastructurii digitale a companiei

Eveniment organizat de ATIC cu suportul GIZ, în cadrul proiectului „Digital Transformation of Small and Medium Enterprises in the Eastern Partnership Countries (DT4SME)".

OBIECTIVUL WORKSHOPULUI

> Workshopul urmărește să ofere participanților o înțelegere practică a principalelor riscuri de securitate informațională care afectează companiile și IMM-urile digitalizate. Participanții vor putea identifica vulnerabilitățile prioritare, vor înțelege măsurile tehnice și organizaționale de bază și vor schița un plan realist de îmbunătățire a securității în propria organizație.

Data	26 august 2026
Ora	De la 12:00
Durata	4 ore, inclusiv pauză
Format	Fizic
Locația	Tekwill, sala Front End
Trainer	Marius Dumitrascu
Structură	Prezentare interactivă + exemple practice + exercițiu de evaluare a riscurilor + sesiune Q&A
Public țintă	Manageri și reprezentanți ai IMM-urilor și companiilor TIC, responsabili IT și securitate, manageri operaționali, responsabili de protecția datelor și angajați implicați în procese digitale

REZULTATE AȘTEPTATE

- Înțelegerea diferenței dintre securitatea informațională și securitatea exclusiv tehnică.
- Recunoașterea celor mai frecvente amenințări: phishing, compromiterea conturilor, ransomware, pierderea sau divulgarea datelor și riscurile generate de furnizori.
- Identificarea activelor și proceselor critice care trebuie protejate.
- Selectarea unui set minim de controale de securitate adecvate dimensiunii și profilului companiei.
- Definirea pașilor de bază pentru reacția la un incident și continuitatea activității.
- Elaborarea unei liste de acțiuni prioritare pentru următoarele 90 de zile.

AGENDA WORKSHOPULUI

01. Deschidere, obiective și evaluarea așteptărilor — 12:00–12:15 (15 min)

- Prezentarea obiectivelor și structurii workshopului.
- Scurt exercițiu de identificare a principalelor preocupări de securitate ale participanților.
- Clarificarea responsabilității comune: management, echipa IT, angajați și furnizori.

02. Peisajul amenințărilor pentru IMM-uri și companii digitale — 12:15–12:55 (40 min)

- Principalele tipuri de incidente care pot afecta activitatea unei companii.
- Phishing, fraudă prin e-mail, compromiterea conturilor și furtul credențialelor.
- Ransomware, pierderea datelor și indisponibilitatea sistemelor.
- Riscuri asociate muncii la distanță, dispozitivelor personale, serviciilor cloud și instrumentelor digitale.
- Riscurile generate de furnizori, parteneri și accesul terților la date sau sisteme.
- Impactul operațional, financiar, juridic și reputațional al unui incident.

03. Evaluarea riscurilor și identificarea activelor critice — 12:55–13:35 (40 min)

- Ce trebuie protejat: date, conturi, sisteme, echipamente, procese și reputație.
- Identificarea proceselor esențiale pentru funcționarea companiei.
- Evaluarea simplificată a riscurilor: amenințare, vulnerabilitate, probabilitate și impact.
- Clasificarea informațiilor și stabilirea nivelurilor de acces.
- Prioritizarea riscurilor în funcție de dimensiunea și resursele organizației.

04. Setul minim de măsuri tehnice și organizaționale — 13:35–14:15 (40 min)

- Autentificarea multifactor, parolele și administrarea conturilor.
- Actualizarea sistemelor, gestionarea vulnerabilităților și protecția dispozitivelor.
- Copii de siguranță, testarea restaurării și separarea backupurilor.
- Controlul accesului și principiul accesului minim necesar.
- Configurarea sigură a e-mailului, serviciilor cloud și instrumentelor de colaborare.
- Politici interne, instruirea angajaților și responsabilități clare.

14:15–14:35 · PAUZĂ · 20 MINUTE

05. Gestionarea incidentelor și continuitatea activității — 14:35–15:15 (40 min)

- Cum recunoaștem și raportăm rapid un posibil incident.
- Primele acțiuni: limitarea impactului, păstrarea informațiilor relevante și escaladarea internă.
- Roluri și responsabilități în timpul unui incident.
- Comunicarea internă și externă și gestionarea relației cu clienții și partenerii.
- Continuitatea activității și recuperarea proceselor critice.
- Analiza post-incident și transformarea lecțiilor în măsuri concrete.

06. Exercițiu practic: planul de securitate pentru 90 de zile — 15:15–15:45 (30 min)

- Participanții selectează un proces digital critic din propria organizație.
- Identificarea activelor, amenințărilor și vulnerabilităților asociate procesului.
- Evaluarea controalelor existente și identificarea principalelor lacune.
- Stabilirea a trei până la cinci acțiuni prioritare, a responsabililor și a termenelor.
- Discuție aplicată și feedback din partea trainerului.

07. Întrebări, concluzii și pași următori — 15:45–16:00 (15 min)

DISCLAIMER

Această activitate este finanțată de Ministerul Federal German pentru Cooperare Economică și Dezvoltare (BMZ) cu implementarea Agenției de Cooperare Internațională a Germaniei (GIZ) în cadrul proiectului „Transformarea digitală a întreprinderilor mici și mijlocii din țările Parteneriatului Estic (DT4SME)”.