GMB
since 1991
COMPUTERS

TRADIȚIE și EXCELENȚĂ în IT & Comunicații

EXPERTUL TĂU ÎN SECURITATE CIBERNETICĂ

DIRECTIVA NIS 2
S.O.C.
DATA CENTER

GMB Computers SRL
Sediul Central:
Str. Traian, nr. 68A,Constanța,
Telefon: +40 241 619 222

GMB Computers
Punct de lucru Cernavodă:
Str. Nicolae Titulescu nr. 4, Cernavodă,
Telefon: +40 241 235 235

Securitatea Cibernetică

Securitatea cibernetică reprezintă un set de practici și tehnologii esențiale pentru asigurarea confidențialității, integrității și disponibilității informațiilor într-un mediu digital, prevenind în același timp amenințările cibernetice precum viruși, hackeri, malware, phishing și atacuri de tip denial-of-service (DoS). Securitatea cibernetică include măsuri de protecție atât pentru infrastructurile IT, cât și pentru datele și sistemele folosite de indivizi, organizații și guverne.

O politică de securitate cibernetică reprezintă un set de principii, reguli și proceduri stabilite de o organizație pentru a proteja sistemele informatice, rețelele și datele împotriva riscurilor și amenințărilor cibernetice.

De ce este necesară securitatea cibernetică în contextul în care tehnologia digitală și internetul sunt parte integrantă a vieților noastre personale și profesionale.

Protecția datelor sensibile: Securitatea cibernetică este esențială pentru a preveni furtul sau divulgarea neautorizată a datelor stocate și prelucrate în sistemul informatic al organizației..

Prevenirea atacurilor cibernetice: Securitatea cibernetică ajută la prevenirea și protejarea împotriva atacurilor precum hacking-ul, phishing-ul, ransomware-ul sau malware-ul care pot provoca daune materiale și morale semnificative.

Menținerea confidențialității și integrității: Securitatea cibernetică asigură că informațiile nu sunt modificate sau accesate de persoane neautorizate, menținându-le integritatea.

Asigurarea continuității afacerii: Securitatea cibernetică ajută la implementarea unor măsuri de protecție și planuri de recuperare în caz de atacuri, asigurând astfel continuitatea afacerilor.

Evoluția tehnologică rapidă: Securitatea cibernetică este necesară pentru a face față noilor riscuri și pentru a proteja rețelele și dispozitivele de ultimele tipuri de atacuri.

Conformitate cu reglementările legale: Securitatea cibernetică ajută organizațiile să îndeplinească cerințele legale, evitând astfel amenzi și sancțiuni.

Măsuri de securitate:

Utilizarea parolelor puternice, criptarea datelor, actualizarea software-ului, utilizarea unui software antivirus cu consolă de management centrală la nivelul organizației și firewall, backup regulat al datelor importante într-un loc sigur și verificarea periodică a backup-urilor, formarea și conștientizarea utilizatorilor în privința celor mai bune practici de securitate cibernetică, controale de acces pentru a asigura că doar persoanele autorizate pot accesa resursele și informațiile sensibile, monitorizarea și auditul activităților, protecția împotriva malware-ului, securizarea rețelelor Wi-Fi, planuri de răspuns la incidente, protecția dispozitivelor mobile

Directiva NIS 2

Directiva NIS2 (Directiva (UE) 2022/2555), legiferată în România de Ordonanța de Urgență nr. 155/2024, este o reglementare europeană esențială pentru creșterea securității cibernetice a rețelelor și sistemelor informatice din Uniunea Europeană. Adoptată în 2022, NIS2 vizează consolidarea protecției infrastructurilor critice și a serviciilor esențiale din statele membre.

Obiectivele NIS2:

1. Îmbunătățirea securității cibernetice a rețelelor și sistemelor informatice

2. Creșterea responsabilității și transparenței

Organizațiile trebuie să fie mai transparente în ceea ce privește gestionarea riscurilor cibernetice, implementarea măsurilor de securitate și raportarea incidentelor de securitate.

3. Creșterea nivelului de colaborare între statele membre ale UE

4. Extinderea domeniului de aplicare

NIS2 extinde domeniul de aplicare la noi sectoare și organizații, inclusiv furnizorii de servicii digitale, cum ar fi piețele online, furnizorii de servicii de cloud și serviciile de calcul în cloud.

5. Măsuri de protecție și gestionare a riscurilor cibernetice
6. Impunerea sancțiunilor și măsurilor de conformitate
NIS2 stabilește sancțiuni pentru organizațiile care nu respectă cerințele de securitate cibernetică, inclusiv amenzi semnificative pentru nerespectarea normelor.
7. Creșterea capacității de răspuns la incidente cibernetice
NIS2 promovează dezvoltarea unor echipe naționale de răspuns la incidente
8. Îmbunătățirea culturii de securitate cibernetică

Conform directivei NIS2 (legiferată în România de OU 155/2024), rolul conducerii executive a organizației este esențial în asigurarea unui cadru de securitate cibernetică eficient și conform cu cerințele reglementărilor.

1. Responsabilitatea globală pentru securitatea cibernetică
Conducerea organizației este direct responsabilă pentru implementarea și menținerea unui sistem de management al securității cibernetice care să fie conform cu cerințele NIS2, și asigură resursele necesare.
2. Stabilirea unui cadru de securitate cibernetică
Managementul organizației trebuie să asigure că securitatea cibernetică este o prioritate, nu doar un obiectiv tehnic, ci și o parte integrantă a culturii organizaționale, prin stabilirea de politici și proceduri clare pentru gestionarea riscurilor cibernetice, evaluarea vulnerabilităților și implementarea măsurilor preventive.
3. Evaluarea și gestionarea riscurilor cibernetice
Responsabilitatea conducerii este de a decide asupra nivelului de risc acceptabil și de a implementa măsuri adecvate pentru a-l reduce.
4. Asigurarea alocării resurselor adecvate
Conducerea are datoria de a aloca suficiente resurse (umane, financiare și tehnologice) pentru a sprijini activitățile de securitate cibernetică.
5. Monitorizarea și raportarea incidentelor de securitate
Conducerea trebuie să asigure implementarea unor mecanisme eficiente de monitorizare a incidentelor de securitate cibernetică.
În cazul unui incident de securitate, managementul este responsabil de răspunsul rapid și eficient.
6. Crearea unui plan de răspuns și recuperare
Managementul este responsabil de coordonarea tuturor acțiunilor de răspuns și de restabilire a funcționalității

Cui se aplică NIS2?

Administrație publică:
Entitățile administrației publice centrale, cu excepția celor din SNAOPSN, instituțiile de învățământ superior, domeniul juridicar, justiție, inclusiv Ministerul Public, ORNISS, Parlamentul României, Guvernul României, Administrația Prezidențială, ASF, BNR și ANCOM

Companii din sectoare critice: energie, transport, sectorul bancar, infrastructuri ale pieței financiare, sectorul sănătății, apă potabilă, ape uzate

Infrastructură digitală, gestionarea serviciilor TIC (business to business)

Spațiu, servicii poștale și de curierat, gestionarea deșeurilor, fabricarea, producția și distribuția de substanțe chimice, producția, prelucrarea și distribuția de alimente, fabricare, furnizori digitali, cercetare

Beneficii pentru utilizatori

- Protecție sporită împotriva atacurilor cibernetice
- Mai multă transparență în gestionarea incidentelor
- Acces la informații și sprijin din partea autorităților competente
- Reducerea riscurilor de pierdere a datelor și compromitere a sistemelor

Concluzii

NIS2 contribuie la securitatea cibernetică pentru toate organizațiile și utilizatorii

Implementarea măsurilor impuse va proteja datele și infrastructurile critice.

Este esențial ca toți actorii implicați să își asume responsabilitatea în aplicarea directivei.

Centrul Operațional de Securitate CYMAROP GMB COMPUTERS

Cu ajutorul SOC-ului CYMAROP GMB Computers, oferă servicii avansate de securitate cibernetică pentru monitorizarea și protejarea infrastructurii IT a clienților.

De asemenea, punem la dispoziție consultanță și asistență pentru conformitatea cu directiva NIS 2.

Servicii oferite:

Monitorizare 24/7 – Supraveghere continuă a echipamentelor critice (de "border" și din interiorul sistemului informatic) pentru a detecta activități suspecte.

Detecție în timp real – Analiză automată a logurilor pentru prevenirea / identificarea și investigarea incidentelor de securitate.

Răspuns rapid – Notificarea imediată a echipelor IT și suport pentru izolarea amenințărilor.

Scanare de vulnerabilități – Teste periodice pentru identificarea și remedierea vulnerabilităților din sistemul informatic.

Suport administrare firewall – Asistență tehnică pentru configurarea și optimizarea securității.

SOC CYMAROP utilizează tehnologii avansate (SIEM, VPN securizat, SNMP/ICMP) pentru a oferi protecție proactivă și conformă cu standardele de securitate.

SERVICII PENTEST - test de securitate realizat pentru a identifica vulnerabilitățile unui sistem IT

Securitatea cibernetică începe cu prevenția.

Contactați-ne pentru protecția infrastructurii dumneavoastră!

FORTINET Synology Bitdefender DELL MikroTik ESET Nessus vmware Jira CISCO

Data Center GMB

Data Center-ul **GMB Computers** oferă infrastructură modernă, securitate avansată și performanță optimizată pentru companii care au nevoie de soluții fiabile de stocare și procesare a datelor.

Infrastructură de ultimă generație

✔ **Climatizare redundantă** – Sistem de răcire eficient pentru menținerea unei temperaturi optime 24/7.

✔ **Generator de tensiune cu UPS tampon redundant** – Continuitate garantată a serviciilor, chiar și în cazul unor întreruperi de energie.

✔ **Securitate fizică și acces controlat** – Supraveghere video, control biometric și acces restricționat.

✔ **Rețea de mare viteză** – Conectivitate redundantă pentru transfer rapid și sigur de date.

✔ **Sisteme anti-incendiu** – Tehnologie avansată pentru prevenirea și stingerea rapidă a incendiilor.

Servicii Data Center

✔ **Colocare echipamente** – Spațiu dedicat pentru serverele clienților, într-un mediu securizat.

✔ **Hosting & Cloud Computing** – Resurse scalabile pentru aplicații și infrastructură IT.

✔ **Backup și Disaster Recovery** – Soluții pentru protecția datelor și continuitatea afacerii.

✔ **Administrare și suport tehnic 24/7** – Monitorizare și intervenție rapidă pentru orice problemă.

GMB Data Center – Performanță, siguranță și disponibilitate non-stop!

AUDITOR NIS ATESTAT DE SECURITATE CIBERNETICĂ LEGEA nr 362/2018

EURO CERT CERTIFIED MANAGEMENT SYSTEM ISO/IEC 27001:2013 00.15.0429

SUN cert CERTIFICATION ISO 9001

SUN cert CERTIFICATION ISO 14001

GMB Computers este o companie specializată în Tehnologia Informației și Comunicațiilor, Centre de Date, Sisteme de Securitate și Securitate Cibernetică. Oferim soluții și echipamente de înaltă calitate, bazate pe tehnologii avansate și inovatoare, alături de servicii de mentenanță și suport tehnic.

GMB Computers - scurt istoric

1991 – Anul înființării. Comercializare/Import de echipamente IT și realizarea primelor rețele structurate de calculatoare în Constanța și nu numai.

1992 – Realizează primul centru expozițional de tehnică de calcul în Constanța.

1993 – Furnizează echipamente IT și periferice pentru numeroase instituții, companii private și persoane fizice.

1994 – Realizează și înregistrează primul calculator compatibil IBM, asamblat în Constanța sub marca înregistrată **GMB Computers.**

1996 – GMB Computers devine primul furnizor de servicii de internet **(ISP)** din Constanța.

1998 – Înființează, alături de Connex, Centrul de excelență **Expert Center Connex** în telefonia mobilă.

1999 – Deschide **Centrul de Instruire în Informatică Dobrogea**, în Constanța și Tulcea – Centru **ECDL**, Centru de testare **VUE, TOEFL, Cambridge.**

2001 – Realizează rețele proprii de **Cablu TV** și devine furnizor de televiziune prin cablu în localități precum **Cernavodă, Bălcescu, Independența, Topraisar, Constanța, Lazu, Mircea Vodă, Saligny, Rasova.**

2003 – GMB Computers este acreditată de ANCOM pentru instalarea de rețele de date și infrastructură în comunicații. Realizează construcții și infrastructuri subterane și supraterane pentru comunicații pe cablu de date/TV, fibră optică sau legături radio.

2004 – Înființează **Centrul autorizat de service** pentru echipamente electronice și **IT Sony, LG, Samsung, Philips, Dell, HP.**

2010 – GMB Computers obține acreditarea **IGPR** pentru proiectare și instalare sisteme de securitate, supraveghere video, control acces, pază perimetrală. Instalează sisteme de securitate și supraveghere cu camere video **CCTV** în instituții, spații industriale și locuințe. De asemenea, instalează porți automate, bariere, bolarzi și turnicheți.

2012 – Realizează **primul Data Center din Constanța,** unde clienții pot înregistra și găzdui site-uri, pot închiria servere virtuale **VPS,** colocaliza serverele proprii, pot închiria spații

GMB since 1991 COMPUTERS

TRADIȚIE și EXCELENȚĂ în IT & Comunicații

pentru salvarea datelor **(cloud storage)**. Data center-ul este dotat cu toate echipamentele și tehnologiile necesare pentru funcționare non-stop, având grup electrogen și UPS pentru protecție împotriva întreruperilor alimentării cu energie electrică

2013 – GMB Computers este certificată **ISO 27001** pentru îndeplinirea standardului în **securitatea informației.** Politicile implementate asigură protecția datelor clienților.

2014 – Este autorizată pentru **proiectarea și instalarea de sisteme de detecție incendiu.**

2019 – Împreună cu **CertDigital,** devine furnizor de **semnătură digitală.**

2020 – GMB Computers devine prestator de servicii **GDPR/DPO,** permițând clienților să externalizeze aceste servicii prin GMB Computers.

2022 – Apariția normelor tehnice de aplicare a legii 362/2018 (NIS) și a Regulamentului pentru atestarea și verificarea auditorilor de securitate cibernetică **NIS (Legea 362)** duce la calificarea specialiștilor GMB Computers în domeniul securității cibernetice, obținând titlul de Auditor de **Securitate Cibernetică,** emis de **DNSC**. GMB Computers dezvoltă această activitate prin **servicii de consultanță, audit și implementarea măsurilor necesare de protecție împotriva atacurilor cibernetice.**

2023 – În completare la infrastructura de **Data Center** și activitatea de **Auditor de Securitate Cibernetică**, GMB Computers **realizează primul Security Operation Center (SOC)** din Constanța, sub denumirea **CYMAROP** (Centrul Operațional, Educațional și de Cercetare în Securitate Cibernetică Maritimă și Operare Autonomă).

În tot acest timp, **GMB Computers** a fost și rămâne un **partener comercial, tehnic și de service** al celor mai mari producători și furnizori din industria IT la nivel mondial, colaborând cu branduri de renume precum **DELL, HP, LENOVO, IBM, SONY, SAMSUNG, CISCO, FORTIGATE, ASUS, XEROX, MINOLTA, AXIS, BOSCH, SCHRACK, LEGRAND** și mulți alții.

Această prezentare evidențiază evoluția GMB Computers de la un furnizor local de echipamente IT la un lider în infrastructura digitală, securitate cibernetică și centre de date.