Bezbednost u digitalnom okruženju

Upravljanje rizicima u deviznom poslovanju i spoljnoj trgovini

Zaštita podataka i transakcija postaje ključno pitanje

- Zaštita podataka i transakcija postaje ključno pitanje, posebno u sektorima kao što su devizno poslovanje i međunarodna trgovina.
- **Podaci o rastu digitalizacije**: Prema izveštajima međunarodnih organizacija kao što su *OECD* i *Svetska trgovinska organizacija (WTO)*, više od 80% kompanija koje se bave međunarodnom trgovinom koriste digitalne alate u svom poslovanju. Digitalizacija ubrzava procese, ali istovremeno povećava izloženost sajber pretnjama.

- **Povezivanje sa spoljnotrgovinskim poslovanjem**:
- Uvođenje digitalnih platformi za plaćanje, e-dokumentaciju i softvere za upravljanje deviznim transakcijama donosi efikasnost, ali i nove rizike.

Digitalne pretnje u spoljnotrgovinskom poslovanju

1. **Sajber napadi**: zvanična predviđanja su da će globalni troškovi povezani sa sajber kriminalom dostići 10,5 biliona dolara godišnje do 2025. godine.

Kompanije koje se bave međunarodnom trgovinom su posebna meta zbog velikih vrednosti transakcija i složenih poslovnih mreža.

2. **Phishing:** Prevare koje imaju za cilj krađu podataka putem lažnih emailova ili sajtova. Phishing je odgovoran za 36% svih sajber napada u poslovnom sektoru

3. **Malveri:** Zlonamerni softveri koji mogu ugroziti sisteme i podatke kompanije. U 2023. godini zabeležen je porast malvera za 25% u odnosu na prethodnu godinu. Ovi malveri često imaju za cilj **krađu finansijskih podataka** ili šifrovanje osetljivih poslovnih dokumenata **u zamenu za otkupninu**

Specifični rizici u deviznom poslovanju

- Devizne transakcije su posebno osetljive na digitalne pretnje zbog svoje prirode i visokih vrednosti koje uključuju.

1. Prevara u platnim nalozima: Lažne instrukcije za plaćanje koje mogu dovesti do gubitka sredstava.

2. Rizik od dvostruke naplate ili lažnih deviznih kurseva: Manipulacije koje mogu rezultirati značajnim finansijskim gubicima.

STRATEGIJE ZAŠTITE I UPRAVLJANJA RIZICIMA

- Efikasne strategije upravljanja rizicima uključuju kombinaciju tehnoloških rešenja, organizacionih mera i pravne zaštite.
- **Tehnološke mere**:
  - **Dvofaktorska verifikacije (2FA)**: *Microsoft* je 2023. godine izvestio da je 2FA sprečilo 99,9% automatskih napada na korisničke račune.

- **Enkripcija podataka**: je jedna od ključnih mera za zaštitu finansijskih podataka, s obzirom da enkriptovani podaci postaju beskorisni ako budu presretnuti.
- **VPN (Virtualne privatne mreže)**: 71% kompanija koristi VPN za zaštitu poslovnih komunikacija, što značajno smanjuje rizik od sajber napada.

Organizacione mere:

- **Obuka zaposlenih**: Prema istraživanju SANS Instituta, kompanije koje redovno obučavaju zaposlene o sajber bezbednosti imaju 50% manje incidentnih slučajeva.

- **Implementacija sigurnosnih politika**: Definisanje jasnih procedura za digitalnu bezbednost koje obuhvataju sve aspekte digitalne bezbednosti, od pristupa podacima do upotrebe mobilnih uređaja.

Pravna zaštita:

- **Ugovorne klauzule o bezbednosti**: Ugovaranje zaštitnih mera sa partnerima u poslovanju.
- **Osiguranje protiv sajber rizika**: Finansijska zaštita u slučaju sajber incidenata.
- Potražnja za sajber osiguranjem porasla za 40% u poslednje tri godine, sa prosečnim pokrićem od 3 miliona dolara po incidentu.

Zaključak

- Ulaganje u digitalnu bezbednost nije samo tehnički, već i strateški prioritet za kompanije koje se bave spoljnom trgovinom i deviznim poslovanjem.
- Neophodno je kontinuirano praćenje digitalnih pretnji i unapređivanje bezbednosnih mera.
- Bezbednost je osnova poverenja u poslovanju.

HVALA VAM NA PAŽNJI

Biljana Trifunović