# Izveštaj o GAP Analizi

## Uvod:

Analizirajući unesene podatke, izveštaj se fokusira na identifikaciju i evaluaciju postojećeg stanja kompanije u odnosu na njene poslovne i sajber bezbednosne strategije, ciljeve, mere i prakse, u cilju otkrivanja gap-ova (praznina) koji bi mogli uticati na postizanje optimalne efikasnosti i sigurnosti.

## Opšta poslovna strategija:

**Pronađeni Gap-ovi:**

1. Revizija poslovne strategije vrši se jednom godišnje, što može biti nedovoljno u brzo promenljivom poslovnom okruženju.

2. Centralizovani sistem za upravljanje zapisima i logovima je samo delimično implementiran, što može predstavljati bezbednosni rizik.

**Preporuke:**

* Povećati učestalost revizije poslovne strategije na polugodišnje ili kvartalno, kako bi se omogućila veća agilnost i prilagođenost promenama.
* Potpuna implementacija centralnog sistema za upravljanje zapismima i logovima za jačanje sajber bezbednosti.

## Sajber bezbednost:

**Pronađeni Gap-ovi:**

1. Kompanija je imala sajber sigurnosni incident u poslednjih godinu dana, što ukazuje na potrebu za poboljšanjem sajber bezbednosnih mera.

2. Iako se sprovode redovne obuke zaposlenih o sajber bezbednosti, dosadašnji incident ukazuje na mogućnost postojanja nedostataka u trenutnoj obuci ili implementaciji politika.

3. Nedostatak učešća u simulacijama sajber napada ili vežbi oporavka može ukazivati na slabiju pripremljenost za stvarne incidente.

**Preporuke:**

* Pregled i pojačanje sajber bezbednosnih treninga za zaposlene, posebno fokusirajući se na identifikaciju i prevenciju specifičnih vrsta sajber napada koji su prethodno zabeleženi.
* Uvođenje redovnih simulacija sajber napada i vežbi oporavka kako bi se poboljšala pripremljenost kompanije za stvarne incidente.
* Razmatranje unapređenja politika BYOD (Bring Your Own Device), kao i jačanje mera za upravljanje pristupima zaposlenih i trećih strana sistemima i podacima.

## Zaključak:

Iako kompanija pokazuje snažnu posvećenost definisanju i implementaciji svoje poslovne strategije i sajber bezbednost, identifikovani gap-ovi ukazują na ključne oblasti za poboljšanje. Povećana frekvencija revizija, kompletiranje implementacije sistema za upravljanje zapisima i logovima, kao i jačanje sajber bezbednosti kroz obuke i simulacije, mogu značajno doprineti efikasnosti i bezbednosti kompanije. Takođe, aktivna težnja ka sticanju sertifikata kao što je ISO 27001 može dodatno unaprediti položaj kompanije kroz dokazivanje posvećenosti najvišim standardima u sajber bezbednosti.

# Predlog za unapređenje poslovanja kompanije

**Na osnovu izveštaja GAP analize i portfolia usluga naše kompanije Positive doo, predlažemo sledeći plan akcija za unapređenje poslovanja i sajber bezbednosti:**

## 1. Periodična revizija poslovne strategije sa sajber bezbednosnim nadogradnjama

**Predlog:**

* Uvesti kvartalne revizije poslovne strategije sa akcentom na integraciju sajber bezbednosnih mera i politika. Ovo će kompaniji omogućiti da agilno reaguje na promene u poslovnom i sajber okruženju, minimizujući tako rizike od bezbednosnih incidenata.

## 2. Implementacija kompletnog sistema za upravljanje zapisima i logovima

**Predlog:**

* Kompletno implementirati centralizovani sistem za upravljanje zapismima i logovima uz podršku najnovijih tehnoloških rešenja iz našeg portfolia, kao što su napredne antivirusne zaštite i next-gen firewall rešenja. Ovo će znatno smanjiti bezbednosne rizike i povećati transparentnost sajber operacija.

## 3. Pojačanje sajber bezbednosnih treninga i simulacija sajber napada

**Predlog:**

* Razviti i sprovesti napredne programe obuke zaposlenih o sajber bezbednosti, posebno fokusirane na najnovije tehnike sajber napada i njihovu prevenciju. Organizovati redovne simulacije sajber napada i vežbe oporavka, koristeći usluge etičkog hakinga i penetration testinga iz našeg portfolia. Ovo će ojačati unutrašnje kapacitete za identifikaciju i odgovor na sajber pretnje.

## 4. Proširenje i jačanje politika BYOD i upravljanja pristupima

**Predlog:**

* Revizija i unapređenje politika BYOD, uključujući jačanje mera za upravljanje pristupima zaposlenih i trećih strana sistemima i podacima. Implementacija najsavremenijih tehnoloških rešenja za autentifikaciju i autorizaciju korisnika pružiće dodatni sloj zaštite, osiguravajući kontrolu pristupa osetljivim informacijama.

## 5. Težnja ka usklađenosti sa regulativama i standardima

**Predlog:**

* Pristupiti procesu sticanja sertifikata ISO 27001, što će osigurati da su sve operacije i procesi usklađeni sa međunarodno priznatim standardima za informacionu sigurnost. Ovo će ujedno povećati poverenje klijenata i partnera u sajber bezbednost kompanije.

## Zaključak i koraci za implementaciju

Predstavljene mere i predlozi su dizajnirani tako da se direktno odnose na identifikovane gap-ove u GAP analizi. Realizacija ovog predloga zahtevaće blisku saradnju između našeg tima u Positive doo i ključnih stakeholdera u vašoj kompaniji. Naš sveobuhvatan pristup sajber bezbednosti garantuje da ćete dobiti najviši nivo zaštite, uz mogućnost da se fokusirate na svoje primarne poslovne aktivnosti, znajući da su vaši podaci sigurni.

Za dalju diskusiju o planu implementacije i personalizovanim rešenjima koje možemo ponuditi vašoj kompaniji, molimo vas da nas kontaktirate. Naš cilj je da vam pružimo mir i sigurnost, oslobađajući vas briga oko sajber pretnji.

