ARBONIA
IT SECURITY

Politika sigurnosti informacija
Politika svesti

Verzija:	1.0
Doneta dana:	13.04.2022. godine
Status:	RELEASED
Klasifikacija:	RESTRICTED
Sastavljena od strane:	CISO
Doneta od strane:	Arbonia IT Board
Smernice:	IS-ISP-GROUP-006 -IT-SECURITY-AWARENESS-POLICY
Revizija:	n/a

Informacije o smernicama

Svrha	Politika svesti opisuje i definiše program podizanja svesti o bezbednosti informacija Arbonia grupe.
Korisnici / primaoci	Svi zaposleni u Arbonia Grupi
Elektronsko odlaganje dokumenata	https://security.arbonia.com

Napomena o promenama

Verzija	Datum	Status	Promena	od strane
0.1	10.01.2022	Draft	Draft of the policy	CISO
0.9	12.04.2022	Draft	Draft for adoption	CISO
0.9	13.04.2022	Review		Arbonia IT Board
1.0	13.04.2022	Adoption		Arbonia IT Board

Sadržaj

Skraćenice

Pojam	Opis
ICT	Informations and Communications Technology (informacione i komunikacione tehnologije)
ISMS	Sistem za upravljanje sigurnošću informacija

Glosar

Pojam	Opis
Sistem za upravljanje sigurnošću informacija	Sistem za upravljanje sigurnošću informacija je niz uspostavljanjenih procedura i pravila unutar organizacije koji služe tome da se trajno definiše, upravlja, kontroliše, održava i kontinuirano poboljšava sigurnost informacija.

1 Svrha, oblast primene i korisnici

Smernica opisuje zahteve i specifikacije programa podizanja svesti o bezbednosti informacija Arbonia grupe i definiše ih kao obavezujuće.

Smernica se odnosi na ceo obim sistema upravljanja bezbednošću informacija (ISMS), odnosno na sve zaposlene u Arbonia Grupi i služi za pojašnjavanje zadataka i zahteva svakog pojedinačnog zaposlenog u zaštiti poverljivosti, integriteta i dostupnosti informacionih sistema i podataka. .

Svi zaposleni u Arbonia Grupi su korisnici i primaoci ove politike.

2 Načela upravljanja

2.1 Važnost programa podizanja svesti o bezbednosti informacija

Zbog sve većeg umrežavanja, digitalizacije i proizašle tehnološke promene, potencijalni napadači otvaraju i dalje mogućnosti za sajber napade. Informaciona bezbednost je veoma dinamična i utiče na skoro svaku oblast Arbonia grupe. Zbog socio-tehničkog aspekta (interakcija između ljudi i informacionog sistema), u ovoj informacionoj mreži mogu se pojaviti slabe tačke.

Pošto se adekvatna zaštita informacija ne može postići samo tehničkim merama, već u velikoj meri zavisi i od ponašanja zaposlenih i njihovog rukovanja podacima i informacionim sistemima, od suštinskog je značaja program podizanja svesti o bezbednosti informacija sa senzibilizacijom i preporukama za akciju u vezi sa sajber pretnjama.

Cilj je da se kod svakog zaposlenog u Arbonia Grupi stvori konstantno rastuća svest o bezbednosti prema motu ***THINK BERFORE YOU Click.Post.Type*** i da to merimo u redovnim intervalima

2.2 Obaveze zaposlenih

Učešće u programu podizanja svesti o bezbednosti informacija je obavezno za sve zaposlene u Arbonia Grupi i mora se sprovoditi savesno i sveobuhvatno. Shodno tome, svi delovi obuke (materijal za obuku i kontrola uspeha) moraju biti završeni.

2.3 Anonimnost / Usklađenost

Kampanje i skladištenje i evaluacija statističkih podataka sprovode se u skladu sa pravnim normama specifičnim za zemlju. Ugovori o zaštiti podataka, ako ih ima, moraju se sklopiti unapred sa odgovarajućim radničkim savetom.

Obrada ličnih podataka se sprovodi samo ako zakonska norma specifične za državu i/ili sporazum pogođenog radničkog saveta to dozvoljava, pri čemu se može konstatovati da obrada ličnih podataka nudi veću dodatnu vrednost, jer se zaposlenima može pružiti ciljana podrška i obuka. Ukoliko zakonska norma ili mišljenje nije dato, mora se obezbediti anonimno prikupljanje i obrada statističkih podataka. Anonimizacija je obezbeđena softverom koji se koristi za phishing i platformu za podizanje svesti. Grupe primalaca treba da budu podeljene u skladu sa specifikacijama anonimizacije.

2.4 Pridošlice/odlasci (ulazak/odlazak) kompanija i zaposlenih

Nova, kupljena (stečena) preduzeća moraju se uzeti u obzir i za sledeću kampanju od trenutka zatvaranja. Ovo važi i za sve novozaposlene. Pored toga, novozaposleni moraju završiti početni kurs obuke o svesti o bezbednosti informacija u roku od 30 dana. Odgovorni IT i HR moraju preduzeti odgovarajuće mere predostrožnosti za ovo. Za zaposlene u prodatim preduzećima učešće je obavezno do trenutka zatvaranja ili do isteka ugovorom ugovorene usluge. U svakom slučaju, međutim, sve dok infrastruktura klijenta ostaje u okviru Arbonia grupe. Izuzeci od ovog pravila moraju biti dogovoreni sa IT menadžerima i CISO-om, a dotični zaposleni moraju biti obavešteni.

3 Program podizanja svesti o bezbednosti informacija

3.1 Definicije

Politika svesti podržava ISMS Arbonia grupe u tome što ova politika na obavezujući način specificira zahteve i specifikacije programa podizanja svesti o bezbednosti informacija. Uz periodične kurseve obuke i provere uspeha, zaposleni su informisani i upoznati sa rizicima i pretnjama po bezbednost informacija, a to ima za cilj da stvori stalnu svest o bezbednosti informacija među svim zaposlenima. Program podizanja svesti o bezbednosti informacija u osnovi se sastoji od dva dela (kampanje):

- Kampanja podizanja svesti
- phishing kampanja

Kampanje se obično sprovode na kvartalnoj osnovi, ali najmanje tri puta godišnje. Fišing kampanje se mogu sprovoditi 6-8 puta godišnje u zavisnosti od potreba i zahteva.

Pored toga, program podizanja svesti o bezbednosti informacija uključuje sledeće mere:

- Poster kampanje
- Alati/softver (dugme Outlook phishing)
- Dodatne kampanje za izložene zaposlene (HR, FI / CO, IT, itd.)

- Dodatne kampanje za zaposlene kojima je potrebna dodatna obuka na osnovu rezultata obuke

Rezultati pojedinačnih kampanja se obrađuju statistički i koriste za kontrolu programa podizanja svesti o bezbednosti informacija.

3.2 Kampanje podizanja svesti

Kampanje podizanja svesti se sprovode prema definiciji i bave se aktuelnim temama koje se odnose na bezbednost informacija.

Kampanje podizanja svesti se sprovode sa centralnom platformom za phishing i podizanje svesti za sve kompanije u Arbonia Grupi i uključuju sledeće tačke:

- Definicija teme podizanja svesti
- Ažuriranje liste primalaca (uključivanje/isključivanje)
- Kreiranje i konfigurisanje kampanje
- Ispitivanje i osiguranje kvaliteta
- Implementacija
- Prikupljanje / obrada statističkih indikatora

Poziv na odgovarajuću kampanju podizanja svesti šalje se direktno zaposlenom putem e-pošte. Poziv je personalizovan i ne može se prosleđivati drugim zaposlenima. Obično se kampanja podizanja svesti sastoji od dva dela, materijala za obuku i kontrole uspeha. U svakom slučaju, svi delovi moraju biti završeni. Pošto je učešće u kampanjama podizanja svesti obavezno za svakog zaposlenog, zaposleni se podsećaju da učestvuju najmanje jednom u toku kampanje podizanja svesti.

3.3 Pecanje kampanja

Pecajuće kampanje se sprovode kako je definisano i bave se simuliranim phishing napadima.

phishing kampanje se sprovode sa centralnom phishing platformom i platformom za podizanje svesti za sve kompanije u Arbonia Grupi i uključuju sledeće tačke:

- Definisanje phishing šablona
- Ažuriranje liste primalaca (uključivanje/isključivanje)
- Kreiranje i konfigurisanje kampanje
- Ispitivanje i osiguranje kvaliteta
- Implementacija
- Prikupljanje / obrada statističkih indikatora

Simulirani phishing napadi se šalju direktno zaposlenom putem e-pošte ili drugim odgovarajućim kanalima. Simulirani phishing napad može imati različite oblike. Ako zaposleni netačno reaguje na simulirani phishing napad, biće automatski obavešten.

3.4 Uloge i odgovornosti

Tim za bezbednost informacija Arbonia grupe odgovoran je za definisanje, pripremu, implementaciju i evaluaciju programa podizanja svesti o bezbednosti informacija. O promenama koje utiču na ceo program razgovara se sa IT odborom i rešava ih CISO.

Lokalni timovi za ljudske resurse su odgovorni za blagovremenu komunikaciju svih kadrovskih promena (ulazak/izlazak/prenos) lokalnom IT timu. Lokalni IT timovi na taj način obezbeđuju aktuelnu bazu podataka (matični podaci zaposlenih u centralnom servisu imenika Active Directori). Grupe primalaca se ažuriraju pre svake implementacije od strane tima za bezbednost informacija Arbonia grupe na osnovu članstva u grupi Active Directori. Lokalni IT tim je takođe odgovoran za uključivanje (početna obuka o svesti o bezbednosti informacija u roku od 30 dana) novih zaposlenih prijavljivanjem novih zaposlenih putem e-pošte na training@arbonia.com. Tim za informacionu bezbednost Arbonia Grupe poziva nove zaposlene na početnu obuku za podizanje svesti po prijemu ove poruke.

4 Odgovornost

Kao što je opisano u poglavlju 2.2, učešće u programu podizanja svesti o bezbednosti informacija je obavezno za sve zaposlene u Arbonia Grupi i mora se sprovoditi savesno i sveobuhvatno. U slučaju ponovljenih kvarova, mogu se definisati dodatne mere obuke. U slučaju suštinskog nepoštovanja ili nedovoljnog učešća, odgovorno rukovodstvo zadržava pravo da preduzme dalje mere.

5 Referenzdokumente

- IS-ISS-GROUP-001-INFORMATION-SECURITY-STRATEGY
- IS-GISP-GROUP-001-GENERAL-INFORMATION-SECURITY-POLICY
- IS-ISP-GROUP-004-IT-SECURITY-POLICY

6 Stupanje na snagu

Ime	Poslovna jedinica	Funkcija	Datum	Potpis
Patrick Langenegger	Corporate IT	CIO Arbonia Group / CIO Division Doors	2021-04-13	n/a
Michael Kreter	Division HVAC	Head of IT Kermi Bereichleiter Informations-verarbeitung	2021-04-13	n/a
Reto Knechtle	Corporate IT	Head of IT Infrastructure	2021-04-13	n/a
Thomas Zehnder	Corporate IT	CISO	2021-04-13	n/a

7 Relevantni prilozi

Br.	Opis	Ime datoteke
1	IS-ISP-GROUP-004-A001-STATEMENT-OF-ACCEPTANCE	IS-ISP-GROUP-004-A001-STATEMENT-OF-ACCEPTANCE