Säkerhet i LAMPORT Larmportalen

– Trygg hantering av din känsliga information

På **Lamport Sweden AB** prioriterar vi säkerheten för våra kunders data. **LAMPORT Larmportalen** är utvecklad med fokus på att skydda känslig information som laddas upp och hanteras i systemet, såsom larmpunkter, konfigurationsinställningar och annan säkerhetsrelaterad data. I detta dokument beskriver vi de åtgärder vi vidtar för att skydda din information, inklusive fysiskt skydd av servrar, kryptering av data, åtkomstkontroll, säkerhetskopiering och skydd mot skadlig programvara.

Vårt mål är att säkerställa att din data alltid är trygg och tillgänglig samtidigt som vi följer de högsta säkerhetsstandarderna.

Fysisk säkerhet av servrar

- **Plats**: Våra servrar är placerade i Stockholm, Sverige i ett datacenter med hög nivå av fysisk säkerhetskontroll.
- **Passersystem & CCTV**
- Access till datacenter hanteras av ett centralt passersystem. All in-/utpassering till våra faciliteter loggas. Samtidigt övervakas alla utrymmen med minst en övervakningskamera.
- **Lås & inbrottslarm**
- Alla utrymmen är larmade och vid intrång larmas väktare direkt. Området ronderas även av väktare utanför kontorstid. Colocation-rackskåp är låsta för access endast av respektive innehavare. Övrig utrustning, som routrar och dedikerade servrar, är placerade på en speciell yta i datacentret som endast behörig personal har tillträde till.
- **Alarm & övervakning**
- Datacentret har en komplett uppsättning av larm som täcker de vanliga larmpunkterna, som klimat och driftlarm. Dessa larm övervakas av lokal personal, men också av Larmcentral.
- Alla områden är skyddade med rökdetektorer. De känsligaste områdena (datahallarna) har samplade detektorer för att upptäcka brand på snabbast möjliga tid. Automatiskt släcksystem (gas) finns även installerat för att skydda elektrisk utrustning i datacentret.

Säker inloggning och åtkomstkontroll

- **Multifaktorautentisering (MFA)**: Om man önskar så kan man ställa krav på Multifaktorsautentisering för inloggning till portalen
- **Rollbaserad åtkomstkontroll (RBAC)**: Åtkomst till känsliga delar av portalen begränsas baserat på användarens roll och behörigheter, vilket säkerställer att endast behöriga användare kan se eller ändra viss data.

Kryptering av data

- **Kryptering under överföring**: All data som överförs till och från LAMPORT Larmportal är krypterad med TLS (Transport Layer Security) för att skydda den under överföring.
- **Kryptering vid vila**: Data som lagras på våra servrar är krypterad enligt industristandard, vilket säkerställer att den förblir skyddad även vid fysisk åtkomst.
- **Hantering av krypteringsnycklar**: Krypteringsnycklar hanteras och lagras säkert, med strikta åtkomstkontroller för att styra vem som kan komma åt och ändra nycklar.

Transaktionsloggning och spårbarhet

- **Revisionsloggning**: All aktivitet i LAMPORT Larmportal loggas, inklusive ändringar i larmkonfigurationer, användaråtkomst och systemuppdateringar. Dessa loggar kan granskas i säkerhetssyfte och för incidenthantering.
- **Åtkomstloggar**: Detaljerade loggar över användaråtkomst, inklusive inloggningsförsök, IP-adresser och sessionstider, registreras och är tillgängliga för granskning.

Redundans och backup

Vi hanterar redundans och säkerhetskopiering för att undvika dataförlust genom:

- **Dataredundans**: Portalen använder redundanta servrar och reservsystem för att säkerställa hög tillgänglighet. Vid hårdvarufel återställs data snabbt och tjänsten fortsätter utan avbrott.
- **Backup av data**: Automatiska säkerhetskopior utförs regelbundet, och dessa säkerhetskopior lagras säkert på flera platser för att skydda mot dataförlust.

Malwareskydd och säker kodning

När det gäller skydd av vår kod och kunddata gentemot skadlig programvara och andra hot så hanteras det enligt nedan:

- **Malwareskydd**: Våra servrar övervakas kontinuerligt för skadlig programvara och andra cyberhot, med proaktiva skanningar och intrångsdetekteringssystem (IDS) för att förhindra skadlig aktivitet.
- **Säkra kodningsprinciper**: LAMPORT Larmportal utvecklas enligt Security Development Lifecycle (SDL) samt följer OWASPs riktlinjer.
- **Regelbundna säkerhetsrevisioner**: Regelbundna säkerhetsgranskningar genomförs av både interna team och externa säkerhetsspecialister för att identifiera och åtgärda potentiella sårbarheter.

Nätverksåtkomst och skydd

Vi säkrar nätverksåtkomst och skyddar systemet från obehöriga intrång genom följande åtgärder:

- **Brandväggsskydd**: All inkommande och utgående trafik filtreras genom brandväggar för att blockera obehörig åtkomst och förhindra attacker.
- **Nätverksåtkomstkontroll (NAC)**: Åtkomst till nätverket som hanterar LAMPORT Larmportal är noggrant kontrollerad, och endast behöriga enheter tillåts ansluta.
- **VPN-skydd**: Säkra VPN-anslutningar används för fjärrhantering av portalen, vilket säkerställer att administratörer kan komma åt systemet på ett säkert sätt.

Framtida uppdateringar och säkerhetsförbättringar

Vi arbetar ständigt för att förbättra säkerheten i portalen.

- **Löpande säkerhetsförbättringar**: I takt med att säkerhetshoten utvecklas, så gör även våra försvarsåtgärder det. Regelbundna uppdateringar av LAMPORT Larmportal säkerställer att systemet förblir säkert och uppdaterat med de senaste branschstandarderna.

Sammanfattning

På Lamport är säkerheten för din data vår högsta prioritet. Med avancerad kryptering, strikta åtkomstkontroller, kontinuerlig övervakning och proaktiv hotdetektering, säkerställer LAMPORT Larmportal att din känsliga information alltid är skyddad.

Kontakta oss för mer information

För mer detaljerad information om våra säkerhetsåtgärder eller för att diskutera specifika frågor, vänligen kontakta oss på kontakt@lamport.se eller ring Per-Olov Wallgren +46 702 429 165