

Data Loss Prevention

MNSEC2017

2017-09-29

Товч мэдээлэл

- Мэдээлэл алдагдахын 64% дотроосоо байдаг
- Ажлаас гарагсдын 50% нь мэдээллээ авч гардаг
- Мэдээлэл алдагдсантай холбоотой зардал өсч байна
- Хууль эрх зүйн асуудал араасаа дагуулдаг

- Data Loss prevention – Мэдээлэл алдагдахаас сэргийлэх
- Data Leak prevention – Мэдээлэл задрахаас сэргийлэх

Мэдээлэл хэрхэн алдагдаж байна

- Дотроос зорилготой ажиллагсад
- Дотоод сэжигтэй ажиллагсад
- Гаднаас

- ХҮНИЙ ТУХАЙ АСУУДАЛ!

Мэдэээллийн 3-н төлөв

- Data in use (endpoint)
- Data in motion (network)
- Data at rest (storage)

Мэдээлэл алдагдах замууд

Хэрэглэгдэж буй мэдээллийн хувьд:

- USB
- Email
- Гар утас, бусад хувийн төхөөрөмжүүд
- HTTPS/HTTP
- IM
- Cloud storage - Google drive, One Drive...
-

Мэдээлэл алдагдах замууд

Дамжигдаж буй мэдээллийн хувьд:

- SMTP
- HTTPS/HTTPS
- IM
- FTP
-

Мэдээлэл алдагдах замууд

Хадгалагдаж буй мэдээллийн хувьд:

- Хадгалалтын алдаа (хамгаалалтгүй, буруу газар гэх мэт)
- Эрхийн зөвшөөрөлгүй хандалт
- Эзэмшигч тодорхойлогдоогүй байх

Байгууллагад үзүүлэх нөлөө

- Санхүүгийн болон нэр хүндийн алдагдал
- Ажиллагсдын болон харилцагчдын мэдээллийн нууцыг алдах
- Өрсөлдөх чадвараа алдах
- Хууль эрх зүйн асуудалд орох

Мэдээллийн ангилах

- Нууцын журам заавар
- Мэдээллийн аюулгүй байдлын бодлого, журам зааврууд
- Эмзэг нууц мэдээлэл гэж юу вэ?
- Эмзэг нууц мэдээллийг хэрхэн ангилах вэ?
- Эмзэг нууц мэдээллийг хэрхэн хамгаалах вэ?

Эрх зүйн баримт бичгүүд

- Төрийн болон албаны нууцын тухай хууль
- Байгууллагын нууцын тухай хууль
- Хувь хүний нууцын тухай хууль

DLP хэрэгслүүд

- Full DLP solution
- Хэсэгчилсэн (Email, Network, I/O хяналт)
- Монголд хэд хэдэн DLP шийдэл орж ирсэн -
AssetView, DeviceLock г.м

Авах арга хэмжээ

- Байгууллагын дотоод хяналтыг сайжруулах -
Журам заавруудыг нэвтрүүлж, мөрдүүлэх
- DLP-ыг аюулгүй байдлын нэг модуль болгон
суулгаж хянах
- Эмзэг нууц мэдээллийг тодорхойлж, тэнд
хандах ашиглах хяналтыг чангатгаж,
хязгаарлалт хийх
- Хөндлөнгийн аудитаар шалгуулах



БАЯРЛАЛАА