БАТЛАВ.
МИАТ ТӨХК-ИЙН
ГҮЙЦЭТГЭХ ЗАХИРАЛ ..... Б.МӨНХТАМИР

2025 оны 3..р сарын 20-ны өдөр

АЖЛЫН ДААЛГАВАР

Аудитын ажлын зорилго:

Мэдээллийн аюулгүй байдлын иж бүрэн аудит, кибер аюулгүй байдлыг эрсдэлийн үнэлгээг холбогдох хууль тогтоомж, дүрэм журам нийцүүлэн хийж зөвлөмж дүгнэлт гаргах.

Аудитын ажлын зарчим:

- Хараат бус, мэргэжлийн байх;
- Мэдээллийн нууцыг чандлан хадгалах;
- Нотолгоонд суурилан үнэлэх
- Мэргэжлийн байр сууринаас хандах;

Мэдээллийн аюулгүй байдлын аудит хийж гүйцэтгэх цар хүрээ:

МИАТ ТӨХК-ийн мэдээллийн технологийн орчинд ажиллаж буй биет болон виртуал сервер, мэдээллийн технологийн тоног төхөөрөмж.

Хийгдэх ажлууд:

Мэдээллийн аюулгүй байдлын аудит хийж гүйцэтгэх ажилд дараах зүйлсийг зайлшгүй багтаах, гэхдээ үүгээр хязгаарлагдахгүй:

- Аюулгүй байдлын бодлого, журам:
  - Байгууллагын аюулгүй байдлын бодлого, журмын хэрэгжилтийг үнэлэх
  - Хууль, дүрэм, стандартын нийцлийг шалгах
    - Кибер аюулгүй байдлын тухай хууль
    - Хүний хувийн мэдээлэл хамгаалах тухай хууль
    - Бусад хууль, тогтоомж, зохицуулалт
  - Ажилчдын сургалт, мэдлэг олгох арга хэмжээг дүгнэх
- Танилт, хандалтын хяналт
  - Хэрэглэгчийн хандалтын удирдлага, баталгаажуулалтын механизм
  - Нэвтрэх эрх, зөвшөөрөл олгох, хүчингүй болгох процессыг шалгах
  - Танилтын системийн аюулгүй байдлыг үнэлэх
  - Байгууллагын хэмжээнд ашиглаж буй систем, сервер сүлжээнд хандалтыг зөв удирдаж буй эсэхийг үнэлэх
- Сүлжээний аюулгүй байдал
  - Сүлжээний аюулгүй байдлыг хангаж буй эсэхийг үнэлэх
  - Сүлжээний аюулгүй байдлыг шалгалт дээр дүгнэлт гаргах
  - Дотоод болон гадаад сүлжээний аюулгүй байдлыг аудит хийх
  - Сүлжээний протоколууд, сүлжээний хяналтын бодлогыг шалгах
  - Төхөөрөмжийн тохиргоог шалгах
- Аюулгүй байдлын шалгалт

- Байгууллагын хэмжээнд аюулгүй байдлын шалгалт хийх процесс бий эсэхийг үнэлэх.
- Эмзэг байдлын үнэлгээ /vulnerability assessment/, нэвтрэлтийн шалгалт /penetration test/ хийдэг эсэхийг шалгах
- Аюулгүй байдлын шалгалтын давтамж, үр дүнтэй байдал, тайлагнал зэргийг шинжлэх

- Бизнесийн тасралтгүй үйл ажиллагаа
  - Байгууллагын хэмжээнд бизнесийн нөлөөллийн дүн шинжилгээ хийж эрсдэлийг тооцсон эсэхийг шалгах
  - Чухал систем, нэгж дээр тасралтгүй үйл ажиллагааг хангах төлөвлөгөө боловсруулан ажиллаж буйг үнэлэх
  - Нөөцлөлт болон нөхөн сэргээх үйл ажиллагаа хийдэг эсэхийг шалгах
  - Тасралтгүй үйл ажиллагааны төлөвлөгөөг турших, холбогдох хүмүүсийг сургах процесс байгаа эсэхийг үнэлэх
- Аюулгүй хөгжүүлэлт (SDLC)
  - Хөгжүүлэлтийн үе шатыг хэрэгжүүлэх процесс бий эсэхийг шалгах
  - Мэдээллийн аюулгүй байдлыг тусгасан байдал, тест хийдэг эсэх болон үүрэг оролцоог тусгаарласан байдлыг шалгах
  - Гуравдагч байгууллагаар хөгжүүлэлт хийлгэх эсхүл програм хангамж болон бусад үйлчилгээг авахад аюулгүй байдлын шаардлага тодорхойлох, хянах процесс байдаг эсэхийг үнэлэх
- Өөрчлөлтийн удирдлага
  - Байгууллагын хэмжээнд өөрчлөлтийн удирдах процесс хэрэгждэг эсэхийг хянах
  - Өөрчлөлтийг ангилах, үүрэг оролцоог тодорхойлох, төлөвлөх, турших, тест хийх зэрэг алхмууд явж буй эсэхийг үнэлэх
- Нөөцлөлтийн удирдлага
  - Нөөцлөлтийн бодлого, сэргээх механизм, шифрлэлт ашиглаж буй эсэх
  - RTO, RPO үзүүлэлтийг тодорхойлж, бодит байдалд нийцэж буй эсэхийг үнэлэх
  - Тест хийдэг эсэхийг шалгах
- Лог бүртгэл
  - Лог бүртгэл, лог хадгалах, аюулгүй байдлыг хангах, стандарт эсхүл хуулийн дагуу хадгалж буй эсэхийг шалгах
  - Лог дээр дүн шинжилгээ хийх процесс, автоматжуулалтын хэрэгжилтийг үнэлэх
- Кибер халдлага, зөрчлийг удирдах
  - Кибер халдлага, зөрчлийг илрүүлэх, мэдээлэх, хариу арга хэмжээ авах, тайлагнах процесс бий эсэхийг шалгах
  - Зөрчлийн үед ажиллах төлөвлөгөө хэрэгждэг эсэхийг шалгах
  - Зөрчил илрүүлэх, хариу үзүүлэх нөөц бий эсэх болон үр дүнтэй хэрэгжиж буйг үнэлэх
- Эрсдэлийн удирдлага
  - Мэдээллийн аюулгүй байдлын эрсдэл үнэлэх, хариу арга хэмжээ авах, монитор хийх алхмууд хэрэгждэг эсэхийг үнэлэх
  - Эрсдэлийн үнэлгээний аргачлал тодорхойлон олон улсын стандарт эсхүл сайн туршлага хэрэгжүүлдэг эсэхийг шалгах
  - Эрсдэлийн үнэлгээг бусад хяналтуудтай уялдуулан үр дүнтэй хэрэгжүүлж буйг үнэлэх
  - Үүрэг хариуцлагыг зөв тодорхойлсон эсэхийг үнэлэх
- Биет аюулгүй байдал

- MNS стандартын дагуу серверийн өрөөний хамгаалалт, хяналтын арга хэмжээг үнэлэх
- Галын хамгаалалт, хяналтын камер, нэвтрэх хяналтын зохион байгуулалт

- Нэвтрэлтийн шалгалт
  - Байгууллагын дотоод болон гадаад сүлжээнд нэвтрэлтийн шалгалт хийж гүйцэтгэх
  - Нэвтрэлтийн шалгалтыг олон улсын стандартын дагуу хийж гүйцэтгэх, тайлагнах
  - Алдааг зассан даруйд дахин шалгалт хийж гүйцэтгэх
  - Нэвтрэлтийн шалгалтыг black box болон gray box хэлбэрээр хийж гүйцэтгэх
  - Нэвтрэлтийн шалгалтын хүрээнд байгууллагад эрсдэл үүсгэж болохуйц үйлдэл хийхгүй байх. Эрсдэлтэй гэж үзсэн тохиолдолд заавал мэдэгдэн эрсдэлийг хамтран үнэлэх.
  - Нэвтрэлтийн шалгалтын хүрээнд ноцтой ангиллын алдаа олдвол шалгалтыг зогсоон мэдэгдэх

Тайлан:

Кибер аюулгүй байдлын аудитын тайлан нь

- ойлгомжтой, цэгцтэй байх
- товч бөгөөд шаардлагатай гол мэдээллүүдийг агуулсан байх
- аудитын үр дүнг бүрэн тусгасан байх
- зөрчилийг арилгах зөвлөмжийг тусгасан байх
- Англи болон Монгол хэл дээр тус тус боловруулсан байх

Хянасан:
Санхүү удирдлагын газрын захирал Н.Цэгц

Боловсруулсан:
Мэдээллийн технологи хөгжүүлэлтийн хэлтсийн
Аюулгүй байдал хариуцсан инженер Ч.Билигсайхан