"Үйлчилгээ тасалдуулах халдлага"-д бэлтгэх ба хариу алхам хийх

Анх нийтлэгдсэн огноо: 2011 оны 9 сар
Хамгийн сүүлд шинэчлэгдсэн огноо: 2025 оны 3 сар

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Te Tira Tiaki
Government Communications Security Bureau

National Cyber Security Centre
PART OF THE GCSB

Танилцуулга

Энэхүү нийтлэлийг Австралийн Радиотехнологийн Газар (ASD), Шинэ Зеландын Үндэсний Цахим Аюулгүй Байдлын Төв (NCSC-NZ), Akamai Technologies Ltd болон Cloudflare Pty Ltd-тай хамтран манай бүс нутагт Үйлчилгээ тасалдуулах (DoS) халдлагын тоо нэмэгдэж байгаатай холбогдуулан боловсруулсан болно. Энэхүү баримт бичиг нь байгууллагуудыг орчин үед тулгарч буй заналхийллийн хандлагад үндэслэн Үйлчилгээ тасалдуулах (DoS) халдлагаас урьдчилан сэргийлэх болон хариу арга хэмжээ авах шилдэг арга туршлагууд бүхий зөвлөмжийг агуулсан.

Мөн энэхүү зөвлөмжийг Австралийн Радиотехникийн Газарын (ASD) дараах нийтлэлүүдтэй хамт уншихыг зөвлөж байна: *Интернэтэд холбогдсон төхөөрөмжүүд (Internet of Things)* ба *Wi-Fi болон раутер*-ээ хэрхэн хамгаалах талаарх нийтлэлүүд. Эдгээр нийтлэлүүд нь хувь хүн санамсаргүйгээр (DoS) халдлагад хувь нэмэр оруулахаас урьдчилан сэргийлэхэд туслах болно.

DoS халдлага гэдэг нь вебсайт, и-мэйл, Домэйн Нэрийн Систем (DNS) зэрэг онлайн үйлчилгээг доголдуулах, ажиллагааг нь сулруулах замаар хууль ёсны хэрэглэгчдийг тэдгээрт хандах боломжгүй болгох зорилготой цахим халдлага юм. Ихэнх тохиолдолд энэ нь тухайн онлайн үйлчилгээг их хэмжээний дата, урсгал эсвэл хүсэлт үүсгэх замаар ачааллыг нь хэтрүүлж, үйл ажиллагааг нь доголдуулах байдлаар хэрэгждэг.

DoS халдлага амжилттай болохын тулд ихэвчлэн тухайн сүлжээн дэх өгөгдлийн урсгал их хэмжээтэй байх шаардлагатай байдаг. Ийм халдлагууд улам бүр түгээмэл болж байгаагийн нэг шалтгаан нь халдлага үйлдэхэд амархан Интернетэд холбогддог (IoT) төхөөрөмжүүдийн тоо улам нэмэгдэж байгаатай холбоотой юм. Интернетэд холбогддог төхөөрөмж (IoT) үйлдвэрлэгчид ихэнхдээ цахим аюулгүй байдлаас илүү хэрэглэгчийн туршлагыг чухалчилдаг тул ухаалаг зурагт, цахилгаан ус буцалгагч, тоос сорогч, хамгаалалтын систем зэрэг энгийн ахуйн хэрэглээний интернэтэд холбогддог төхөөрөмжүүд нь эмзэг, халдлагад өртөмтгий байх тохиолдол элбэг байдаг. Эдгээр төхөөрөмжүүдийг ихэвчлэн алсын зайнаас гэмт этгээдүүд хяналтдаа оруулж, олон тооны төхөөрөмжүүдээс бүрдсэн “ботнет” сүлжээг үүсгэж, сүлжээгээр их хэмжээний урсгал үүсгэдэг. Үүний үр дүнд өрх болон байгууллагууд өөрсдөө мэдэлгүйгээр DoS халдлагыг хэрэгжүүлэх боломжтой дэд бүтцийн сүлжээг бий болгоход хувь нэмэр болдог.

Сүүлийн үед өрнөж буй явцаас харахад, халдагчид олон тооны Интернэтэд холбогддог төхөөрөмжүүдийг эзэмшиж авсны дараа энэхүү дэд бүтцийг цахим гэмт хэрэгтнүүд болон халдлага үйлдэгч нарт түрээслэх эсвэл зарах тохиолдол нэмэгдэж байна. Тэдгээр нь өөрсдийн зорилгод нийцсэн DoS халдлагыг уг дэд бүтцээр дамжуулан хийх сонирхол ихсэж байгаа. Ихэнх тохиолдолд DoS халдлагыг байгууллага компаниудын бүтээмжийг бууруулах, санхүүгийн алдагдалд хүргэх, эсвэл өөр бусад тодорхой зорилгын төлөө олон нийтийн анхаарлыг татах зорилгоор хийдэг. Австралийн Радиотехникийн Газарын (ASD) зөвлөмжид *Бүгд Найрамдах Хятад Улстай холбоотой этгээдүүд роутер болон Интернэтэд холбогддог төхөөрөмжүүдийг ботнет ажиллагаанд ашигласан талаар* энэхүү үйл ажиллагааны жишээ болгон дурдсан болно.

Манай эдийн засаг илүү цахим хэлбэрт шилжиж, интернэтэд холбогдсон хамгаалалт муутай төхөөрөмжийн тоо нэмэгдсээр байгаатай холбогдуулан DoS халдлагууд цаашид ч өссөөр байх төлөвтэй байна.

Байгууллагын онлайн үйлчилгээг доголдуулах эсвэл ажиллагааг нь сулруулах зорилгоор халдагчид хэд хэдэн аргыг ашигладаг бөгөөд үүнд:

- Их хэмжээний шаардлагагүй сүлжээний томоохон урсгалыг онлайн үйлчилгээ рүү илгээн уг сүлжээний бүх хүчин чадлыг эзэгнэх оролдлого.
- Онлайн үйлчилгээнд зориулж оновчтой тохируулсан сүлжээний урсгал үүсгэж, тухайн компьютерын тооцоолох нөөцийг шавхах оролдлого.
- Олон компьютер, IoT төхөөрөмж эсвэл бусад интернэтэд холбогдсон төхөөрөмжүүдийг ашиглан сүлжээний урсгалыг тухайн сүлжээ рүү олон чиглэлээс, илүү том цар хүрээтэйгээр чиглүүлэх. Үүнийг тархмал халдлага (DDoS халдлага) гэж нэрлэгддэг DoS халдлагын түгээмэл төрөл юм.
- Байгууллагын домэйн бүртгэл эсвэл DNS серверүүдийг хууль бус байдлаар эзэмшиж, хууль ёсны хэрэглэгчдийг тухайн байгууллагын онлайн үйлчилгээнээс таслах оролдлого.

Байгууллагууд DoS халдлагад өртөхөөс бүрэн зайлсхийж чадахгүй ч, ийм халдлагад бэлэн байх, халдлагын сөрөг нөлөөг нь багасгахын тулд хэрэгжүүлэх боломжтой хэд хэдэн арга хэмжээ байдаг. DoS халдлагаааас урьдчилан сэргийлэх нь хамгийн сайн стратеги юм. Учир нь халдлагад бэлтгээгүй бол халдлага болсон хойно хариу арга хэмжээ авах нь хэцүү бөгөөд үр дүн муутай байдаг.

Байгууллагууд голчлон өөрсдийгөө DoS халдлагаас хамгаалахад анхаардах ёстой ч эргээд өөрсдийн онлайн үйлчилгээ болон интернэтэд холбогдсон төхөөрөмжүүдийг халдагч нарт ашиглах боломжгүй болгох зорилго бүхий хамгаалах арга хэмжээнүүдийг авах хэрэгтэй.

DoS халдлагад бэлтгэх

Манай бүс нутагт DoS халдлагын тоо өсч байгаатай холбогдуулан DoS халдлагад бэлтгэх аливаа арга хэмжээ авахын өмнө танай байгууллага өөрсдийн бизнесийн үйл ажиллагаанд үнэлгээ хийж, DoS халдлагын үед танай онлайн үйлчилгээнүүд бүгд бүрэн ажиллах байх ёстой эсэх, эсвэл зарим онлайн үйлчилгээ түр хугацаагаар тасалдах нь боломжтой эсэхийг тодорхойлох хэрэгтэй.

Хэрэв танай байгууллага өөрийн DoS халдлагыг эсэргүүцэх чадвараа нэмэгдүүлэхийг хүсвэл DoS халдлага гарахаас өмнө боломжит хийгээд практикт нийцсэн дараах арга хэмжээг идэвхтэй авч хэрэгжүүлэх хэрэгтэй.

- Хэрэв танай байгууллага контент түгээх сүлжээ (CDN) ашиглаж байгаа бол өөрийн нөөц бололцоо болон практикт нийцсэн дараах нэмэлт арга хэмжээг хэрэгжүүлэх хэрэгтэй.
  - Танай үндсэн веб серверийг янз бүрийн программ хангамж болон сүлжээний түвшний халдлагаас хамгаалах боломж бүхий функцтэй CDN ашиглахыг зорих. Зарим CDN-үүд веб программын галт хана (web application firewall) болгон эдгээр функцүүдийг оруулсан байдаг.
  - Үндсэн веб серверийн Интернэт протокол (IP) хаягийг хэрэгцээгүйгээр олон нийтэд ил гаргахгүй байхыг хичээгээрэй, мөн олон нийтэд ил болсон тохиолдолд DoS халдлагаас хамгаалахыг чухалчилна уу.
  - Халдагчид таамаглах боломжтой IP хаягийг үндсэн веб сервертээ ашиглахаас зайлсхийх хэрэгтэй. Жишээ нь танай онлайн үйлчилгээнүүдийн олон нийтэд ил болсон IP хаягтай ижил сүлжээний дэд сүлжээнд (subnet) байгаа IP хаяг гэх мэт.
  - Сүлжээний хандалтын хязгаарлалт (файрвол гэх мэт) ашиглан зөвхөн CDN болон танай байгууллагын зөвшөөрөгдсөн удирдлагын сүлжээнүүд л танай үндсэн веб серверт хандах боломжтой байлгаарай.
  - Хэрэв байгууллагын үндсэн веб серверийн хамгаалалтыг өндөр түвшинд байлгах шаардлагатай бол өөрийн үндсэн веб сервер болон CDN үйлчилгээ үзүүлэгчийн хоорондох хувийн сүлжээ зэрэг тэсвэртэй, олон талт сүлжээний холболтыг ашиглаж болох эсэхийг бодолцоорой.
  - CDN, үндсэн веб сервер болон хэрэглэгчийн HTTP толгой хэсгүүдийг тохируулан хадгалагчийн (caching) хэмжээг оновчтой болгоорой.
  - Хэрэв илүү өндөр түвшний үйлчилгээний тасралтгүй байдал шаардлагатай байдаг бол эрсдэл багатай IP хаягуудын хүсэлтийг эрсдэл өндөртэй IP хаягуудын хүсэлтээс тусад нь боловсруулахын тулд эх веб серверүүдийг салгаж ашиглахыг авч үзээрэй.
- Танай онлайн үйлчилгээний хууль ёсны хэрэглэгчдэд танай ямар үйл ажиллагаа, үйлчилгээний чанар хүлээн зөвшөөрөгдөх, тэдгээрийг хэрхэн хадгалах, мөн DoS халдлагын үед ямар үйл ажиллагаа шаардлагагүй болохыг тодорхойлно уу.
- Үүлэн технологид суурилсан DoS халдлагаас хамгаалах үйлчилгээг ашиглах, хэрэгжүүлэх.
- Танай байгууллагын халдлагад өртөх магадлалыг багасгахын тулд дараах арга хэмжээг авах боломжтой:
  - DoS халдлагыг эсэргүүцэх чадвартай нэр хүндтэй үйлчилгээ үзүүлэгч гуравдагч компаниас үндсэн онлайн үйлчилгээгээ (жишээ нь, DNS)-г авах.
  - И-мэйл зэрэг онц чухал онлайн үйлчилгээнүүдийг халдлагад илүү өртөмтгий бусад онлайн үйлчилгээнүүдээс (вебсайтууд гэх мэт) тусад нь салгах.
  - DoS халдлагыг саармагжуулах/хаах үйлчилгээ нь зөвхөн тухайн онлайн үйлчилгээний сүлжээний порт(ууд)-той холбоотой урсгалыг зөвшөөрдөг байх.
- Үйлчилгээ үзүүлэгчидтэйгээ DoS халдлагыг урьдчилан сэргийлэх болон саармагжуулах стратегийнх нь талаар, ялангуяа дараах асуудлуудаар ярилцвал зохино:
  - Дэлхийн аль ч хэсгээс ирж болох DoS халдлагыг эсэргүүцэх батлагдсан чадавхитай эсэх
  - DoS халдлагыг амжилттай даван туулж байсан, мөн DoS халдлагын эсрэг цогц туршилтыг гүйцэтгэж байсан туршлагатай эсэх
  - Сүлжээний урсгалыг гар аргаар шинжлэх гэх мэт хүний оролцоогүйгээр DoS халдлагын ихэнх төрлийг автоматаар саармагжуулах чадвартай эсэх

  - Үйлчилгээний үнэ тогтвортой эсэх, эсвэл ашигласан сүлжээний урсгалыг болон компьютерын хүчин чадлын хэмжээнээс хамааралтайгаар үнэ өөрчлөгддөг эсэх, мөн боломжит төлбөрийн дээд хязгаарыг тогтоох боломжтой эсэх зэрэг үнэ төлбөрийн бодлого болон арга барилыг тодруулах
  - DoS халдлагын үед онлайн үйлчилгээгээ түр зогсоох, халдлагын талаар танд мэдэгдэл өгөх тал дээр тодорхой бодлого тодорхойлсон байдаг эсэх
  - DoS халдлагын үед урьдчилан бэлдсэн, зөвшөөрөгдсөн арга хэмжээ авах боломжтой эсэх
  - Интернэт үйлчилгээ үзүүлэгчидтэйгээ DoS халдлагаас урьдчилан сэргийлэх тохиргоо, гэрээ хэлэлцээрүүд хийгдсэн эсэх.
- DoS халдлагыг илрүүлэх төлөвлөгөөт арга хэмжээ байдаг эсэх. Үүнд системийн нөөцийн хүртээмж, сүлжээний урсгал, компьютерын хүчин чадлын нөөц, холбогдох зардлын бодит цагийн хяналт болон анхааруулга өгөх системүүд багтана.
- DoS халдлагын үед үйлчилгээ тасалдахаас сэргийлэн хамгийн бага боловсруулалт, болон бага хэмжээний сүлжээний урсгал шаардагдах статик вебсайтын хувилбарыг бэлтгээрэй.
- Их хэмжээний сүлжээний урсгал, хангалттай компьютерын хүчин чадлын нөөц, газар зүйн хувьд тарсан байрлалтай хостинг үйлчилгээ, мөн үүлэн технологид суурилсан урсгал шүүлтүүр бүхий өндөр тэсвэртэй онлайн үйлчилгээг авах, ашиглахыг зөвлөж байна. Үүнд ихэвчлэн нэр хүндтэй CDN ашиглан статик веб контентыг хадгалах болон үндсэн веб серверийг шаардлагагүй сүлжээний урсгалаас хамгаалах зэрэг багтана.
- Танай байгууллагын домэйн нэрийг хамгаалахын тулд домэйн бүртгэлийг түгжих (registrar locking) үйлчилгээг ашиглаж, домэйн бүртгэлийн холбоо барих мэдээлэл болон бусад мэдээлэл зөв эсэхийг шалгаж, мөн ASD-ийн *Домэйн нэрийн систем (DNS)-ийн аюулгүй байдал* гарын авлагад заасан нэмэлт зөвлөмжийг дагаарай.
- Үйлчилгээ үзүүлэгчдийнхээ холбоо барих мэдээллийг шинэчилж, байгууллагынхаа холбоо барих мэдээллийг тэдэнд цаг тухайд нь өгч байгаарай. Ингэснээр танай байгууллагын шаардлагын дагуу, жишээ нь 7 хоногийн 24 цагийн турш гэх мэтээр холбогдох боломжтой байна.
- Энгийн харилцаа холбооны сувгууд ажиллахгүй болсон үед үйлчилгээ үзүүлэгч байгууллагдаа итгэмжлэгдсэн, найдвартай харилцааны хэрэгсэл болох танай байгууллагын энгийн сүлжээнээс гадуурх (out-of-band) холбоо барих мэдээллийг өгөх
- Өөрийн онлайн үйлчилгээ болгонд таарсан, төрөл бүрийн DoS халдлагын үед хэрэгжүүлэх цахим аюулгүй байдлын хариу арга хэмжээ авах төлөвлөгөөг боловсруулж, хэрэгжүүлж, тогтмол (жилд дор хаяж нэг удаа) туршиж, байнга шинэчилж байх
- Нэмэлт тооцооллын нөөц ихээр шаарддаг эсвэл нэмэлт санхүүгийн зардал (жишээлбэл, SMS илгээх зэрэг) үүсгэдэг, хамгийн ихээр халдлагад өртдөг функцүүдийг хамгаалахаар программ хангамжийн бүтцийг төлөвлөх.
  - Хамгаалалтын арга хэмжээнд хандалтын давтамжид хязгаарлалт хийх, ирсэн хүсэлтүүдийг хүн биечлэн гаргасан эсэхийг баталгаажуулах зэрэг орно.
  - Мөн программын үйл ажиллагааны хүрээнд байх ёсгүй урсгалыг онилсон DoS халдлагын тест хийх мэтээр DoS халдлагын тестүүдийг хийж гүйцэтгэх
  - DoS халдлагын боломжит сувгуудыг илрүүлж, арилгах зорилгоор илүү өргөн хүрээтэй ачааллын тест хийх.

DoS халдлагын үед авах арга хэмжээ

Хэрэв танай байгууллага DoS халдлагад урьдчилан бэлтгэл хийгээгүй бол дээр дурдсан зарим арга хэмжээг халдлагын үед хэрэгжүүлэхийг оролдож болно. Гэсэн хэдий ч эдгээр арга хэмжээ нь үр дүн багатай байх магадлалтай бөгөөд хэрэгжүүлэхэд их хугацаа шаардсанаар танай байгууллагын хариу үйлдэл үзүүлэх чадамжийг бууруулж болзошгүй юм.

Тохиромжтой болон боломжтой бол дараах арга хэмжээг танай байгууллага DoS халдлагын үед хэрэгжүүлвэл зохино.

- Цахим аюулгүй байдлын тохиолдлын хариу арга хэмжээ авах төлөвлөгөөгөө хэрэгжүүлэх.
- Үйлчилгээ үзүүлэгч байгууллагаас шууд хариу арга хэмжээ авч чадах эсэхийг тодруулж асуугаарай. Хэрэв өмнө нь тэдний хариу үйлдэл үзүүлэх чадамжийн талаар ярилцаж байгаагүй бол, тэд ийм арга хэмжээ авах боломжгүй, эсвэл хүсэхгүй байх магадлалтайгаас гадна нэмэлт төлбөр шаардах нөхцөл байж болзошгүйг анхаарах хэрэгтэй.
- Одоогийн DoS халдлагыг улам үр дүнтэй болгож буй, чухал биш функцүүдийг хаах эсвэл онлайн үйлчилгээнээсээ чухал бус агуулгыг устгах хэрэгтэй. Жишээ нь, хайлтын функцгүй, динамик агуулгагүй эсвэл том хэмжээтэй файлгүй вебсайтын хувилбарыг нэвтрүүлэх.
- Өөрийн үйлчлүүлэгчид болон үйлчилгээ үзүүлэгч, харилцагч байгууллага, түүний дотор DoS халдлагыг сааруулах үйлчилгээ үзүүлэгчтэйгээ тогтмол харилцаа холбоог хадгалах. Мөн онлайн үйлчилгээнийхээ хүртээмжийг тасралтгүй хянаж байх.
- Хэрэв таны үндсэн веб сервер шууд халдлагад өртөж байвал IP хаягаа солих талаар бодох хэрэгтэй бөгөөд хамгаалалтын арга хэмжээ авч амжаагүй байхад шинэ IP хаягаа олон нийтэд ил зарлахгүй байхыг анхаарна уу.
- DoS халдлагыг холбогдох байгууллагуудад мэдээлэх, үүнд энэхүү нийтлэлийн “Холбоо барих мэдээлэл” хэсэгт заасан ASD болон NCSC-NZ байгууллагууд багтана.

DoS халдлагад санамсаргүйгээр хувь нэмэр оруулахгүй байх

Танай байгууллага бусдад сөргөөр нөлөөлж болох DoS халдлагад санаандгүй оролцохоос сэргийлж дараах арга хэмжээг хэрэгжүүлвэл зохино.

- Шаардлагагүй, аюулгүй байдал нь хангагдаагүй эсвэл хангалтгүй засвар үйлчилгээ хийгдээгүй онлайн үйлчилгээ, IoT төхөөрөмж болон бусад интернэтэд холбогддог төхөөрөмжүүдийг олон нийтэд ил гаргахгүй байх.
- Интернэтэд ил байдаг үйлчилгээ, IoT төхөөрөмж болон бусад интернэтэд холбогдсон төхөөрөмжүүдийг аюулгүйгээр тохируулж, засварлаж, байнга хянах.
  - Жижиг бизнесүүдэд зориулсан нэмэлт зөвлөмжийг ASD-ийн *Интернэтэд холбогдсон төхөөрөмжүүд* болон *Wi-Fi болон раутерийг аюулгүй байлгах* нийтлэлүүдээс авна уу.

Хэрэв танай байгууллага онлайн үйлчилгээ эрхэлж байгаа бол дараах нэмэлт арга хэмжээг хэрэгжүүлвэл зохино.

- АНУ-ын Цахим аюулгүй байдал ба дэд бүтцийн аюулгүй байдлын агентлаг (CISA)-ийн *UDP-д суурилсан хүч нэмэгдүүлсэн халдлагын* талаарх зөвлөмжийг тэргүүн ээлжинд авч үзэх.
- Шинээр илэрч буй хүч нэмэгдүүлсэн халдлагын сувгуудыг тогтмол хянаж, онлайн үйлчилгээнүүдээ тэдгээрээс хамгаалах арга хэмжээг авах.
- Оруулж ирэх ба гадагш гаргах сүлжээний хандалтын хяналтуудыг тохируулж, зөвшөөрөгдсөн онлайн үйлчилгээ болон байгууллагуудад л хандалт олгохыг хязгаарлах.
- Хүч нэмэгдүүлсэн халдлагад өртөмтгий онлайн үйлчилгээнд нууц хаягаас ирэх хандалтуудыг шаардлагагүй бол хаах.
- Хандалтыг хянах/хаах боломжгүй эсвэл тохиромжгүй үед хэрэглэх хэрэглээний зөрчлөөс болж үүсэх үр дагаврыг бууруулах зорилгоор хандалтын давтамж-хязгаарлах механизмыг хэрэгжүүлэхийг авч үзэх.

Нэмэлт мэдээлэл

ASD-ийн *Мэдээллийн аюулгүй байдлын гарын авлага* нь байгууллагуудын систем, өгөгдлийг цахим эрсдэлээс хамгаалахад ашиглаж болох цахим аюулгүй байдлын бодлого зөвлөмж юм. *Цахим аюулгүй байдлын тохиолдлыг саруулах стратегиуд* болон Гол найман зарчим нь энэхүү зарчимтай уялддаг.

Шинэ Зеландын Мэдээллийн Аюулгүй Байдлын Гарын Авлага нь Шинэ Зеландын Засгийн Газрын мэдээллийн баталгаажуулалт болон мэдээллийн системийн аюулгүй байдлын гарын авлага юм. Энэ нь байгууллагын мэдээллийн аюулгүй байдлын удирдлагууд болон байгууллагуудад үйлчилгээ үзүүлдэг нийлүүлэгчид, гэрээт ажилтнууд, зөвлөхүүдийн хэрэгцээг хангахаар зориулсан практик гарын авлага юм.

DoS халдлагын төрөл бүрийн талаарх дэлгэрэнгүй мэдээллийг CISA-ийн *DDoS Тургэн Гарын Авлага* болон *Тархмал Үйлчилгээг Тасалдуулах Халдлагыг Ойлгох, Хариу арга хэмжээ авах нь* нийтлэлүүдээс авна уу.

Холбоо барих мэдээлэл

Австралид энэ зөвлөмжийн талаар асуулт байвал *ASD*-д бичгээр хандах эсвэл 1300 CYBER1 (1300 292 371) дугаар руу залгаарай.

Шинэ Зеландад цахим аюулгүй байдлын тохиолдлыг мэдээлэхийг хүсвэл incidents@ncsc.govt.nz хаягаар имэйл илгээх эсвэл NCSC-NZ-ийн Халдлагын тохиолдлыг мэдээлэх веб хуудсанд зочлоно уу.

Хариуцлагаас татгалзах мэдэгдэл

Энэхүү гарын авлага нь ерөнхий мэдээлэлд зориулагдсан бөгөөд хууль зүйн зөвлөгөө биш юм. Тодорхой нөхцөл байдал, яаралтай үед энэхүү мэдээлэлд бүрэн найдаж болохгүйг анхаарна уу. Чухал асуудал гарсан тохиолдолд өөрийн нөхцөл байдалд тохирсон бие даасан мэргэжлийн зөвлөгөө авахыг зөвлөж байна.

Энэхүү гарын авлагад агуулагдсан мэдээлэлд үндэслэн хийсэн аливаа үйлдлээс улбаалсан аливаа хохирол, алдагдал, зардлыг Холбооны улс хариуцахгүй.

Дэлгэрэнгүй мэдээлэл авах эсвэл цахим аюулгүй байдлын зөрчлийн тохиолдлыг мэдээлэх бол бидэнтэй холбогдоно уу:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Энэ дугаарыг зөвхөн Австралийн дотор ашиглах боломжтой.

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre