ການກຽມພ້ອມ ແລະ ການຕອບສະໜອງ ຕໍ່ການໂຈມຕີແບບປະຕິເສດການບໍລິການ

ຈັດພິມມາຄັ້ງທຳອິດ: ເດືອນກັນຍາ 2011
ອັບເດດຫຼ້າສຸດ: ເດືອນມິນາ 2025

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

ການແນະນຳ

ເອກະສານເຜີຍແຜ່ນີ້ໄດ້ຮັບການພັດທະນາໂດຍສຳນັກງານສັນຍານອົດສະຕາລີ (ASD) ຮ່ວມມືກັບສູນຄວາມປອດໄພທາງໄຊເບີ ແຫ່ງຊາດຂອງນິວຊີແລນ (NCSC-NZ), Akamai Technologies Ltd ແລະ Cloudflare Pty Ltd, ເພື່ອຕອບສະໜອງ ຕໍ່ທ່າອ່ຽງທີ່ເພີ່ມຂຶ້ນໃນການໂຈມຕີແບບປະຕິເສດການບໍລິການ (DoS) ໃນພາກພື້ນຂອງພວກເຮົາ. ມັນໃຫ້ຄຳແນະນຳກັບອົງກອນ ຕ່າງໆ ກ່ຽວກັບແນວທາງປະຕິບັດທີ່ດີທີ່ສຸດໃນການບັນເທົາໄພຂົ່ມຂູ່ໃນປະຈຸບັນ ເພື່ອກຽມພ້ອມ ແລະ ຕອບສະໜອງຕໍ່ການໂຈມຕີ ແບບ DoS.

ພວກເຮົາແນະນຳໃຫ້ອ່ານຄຳແນະນຳນີ້ຮ່ວມກັບ *ອຸປະກອນອິນເຕີເນັດຂອງສິ່ງຕ່າງໆ* ຂອງ ASD ແລະ *ຮັກສາຄວາມປອດໄພ ອຸປະກອນ Wi-Fi ແລະ ເຣົາເຕ* ຂອງທ່ານ. ສິ່ງພິມເຫຼົ່ານີ້ຊ່ວຍໃຫ້ບຸກຄົນຕ່າງໆຫຼີກລ່ຽງການມີສ່ວນຮ່ວມໃນການໂຈມຕີ DoS ໂດຍບໍ່ໄດ້ຕັ້ງໃຈທີ່ສາມາດສົ່ງຜົນກະທົບຕໍ່ຄົນອື່ນໄດ້.

ການໂຈມຕີ DoS ແມ່ນການໂຈມຕີທາງໄຊເບີທີ່ອອກແບບມາເພື່ອລົບກວນ ຫຼື ທຳລາຍການບໍລິການອອນລາຍເຊັ່ນ: ເວັບໄຊທ໌, ອີ ເມວ ແລະ ບໍລິການລະບົບຊື່ໂດເມນ (DNS), ເພື່ອປະຕິເສດການເຂົ້າເຖິງຂອງຜູ້ໃຊ້ທີ່ຖືກຕ້ອງຕາມກົດໝາຍ. ໂດຍປົກກະຕິນີ້ແມ່ນ ບັນລຸໄດ້ໂດຍການເຮັດໃຫ້ການບໍລິການທາງອອນລາຍທີ່ມີຂໍ້ມູນ, ການເຊື່ອມຕໍ່ ຫຼື ການຮ້ອງຂໍເພື່ອທຳລາຍບໍລິການ ແລະ ຫຼຸດ ປະສິດທິພາບຂອງບໍລິການ.

ໂດຍທົ່ວໄປແລ້ວ ການໂຈມຕີແບບ DoS ຕ້ອງໃຊ້ປະລິມານການຮັບສົ່ງຂໍ້ມູນໃນເຄືອຂ່າຍຈຳນວນຫຼາຍເພື່ອໃຫ້ປະສົບຜົນສຳເລັດ. ພວກມັນກຳລັງກາຍມາເປັນເລື່ອງທຳມະດາຫຼາຍຂຶ້ນ, ສ່ວນໜຶ່ງເນື່ອງມາຈາກມີອຸປະກອນອິນເຕີເນັດຂອງສິ່ງຕ່າງໆ (IoT) ທີ່ຖືກ ທຳລາຍໄດ້ງ່າຍຂຶ້ນ. ເນື່ອງຈາກຜູ້ຜະລິດ IoT ມັກຈະໃຫ້ຄວາມສຳຄັນຕໍ່ປະສົບການຂອງຜູ້ໃຊ້ຫຼາຍກວ່າຄວາມປອດໄພທາງໄຊເບີ, ອຸປະກອນທີ່ມີຄວາມສ່ຽງອາດລວມມີເຄື່ອງໃຊ້ໃນຄົວເຮືອນທົ່ວໄປທີ່ເຊື່ອມຕໍ່ອິນເຕີເນັດ ເຊັ່ນ: ໂທລະພາບອັດສະລິຍະ, ກາຕົ້ມນ້ຳ, ເຄື່ອງດູດຝຸ່ນ ແລະ ລະບົບຮັກສາຄວາມປອດໄພ. ອຸປະກອນເຫຼົ່ານີ້ມັກຈະຖືກທຳລາຍຈາກໄລຍະໄກໂດຍຜູ້ບໍ່ປະສົງດີເພື່ອສ້າງ ‘ບ໊ອດ ເນັດ’ ຂອງອຸປະກອນ ເພື່ອໃຊ້ສ້າງການຈະລາຈອນເຄືອຂ່າຍນີ້, ເຊິ່ງສາມາດສົ່ງຜົນໃຫ້ຄົວເຮືອນ ແລະ ອົງກອນມີສ່ວນສະໜັບສະໜູນ ໂຄງສ້າງພື້ນຖານທີ່ເປີດໂອກາດໃຫ້ເກີດການໂຈມຕີແບບ DoS ໂດຍບໍ່ໄດ້ຕັ້ງໃຈ.

ກິດຈະກຳທີ່ຜ່ານມາຊີ້ໃຫ້ເຫັນວ່າເມື່ອຜູ້ບໍ່ປະສົງດີເຈາะລະບົບອຸປະກອນ IoT ຈຳນວນຫຼວງຫຼາຍແລ້ວ, ເຂົາເຈົ້າອາດຈະເຊົ່າ ຫຼື ຂາຍໂຄງ ສ້າງພື້ນຖານນີ້ໃຫ້ກັບພວກອາດຊະຍາກຳທາງໄຊເບີ ແລະ ແຮັກເກີ, ເຊິ່ງສົນໃຈທີ່ຈະທຳການໂຈມຕີແບບ DoS ຕໍ່ກັບເປົ້າໝາຍທີ່ຕົນ ເລືອກຫຼາຍຂຶ້ນເລື້ອຍໆ. ໃນກໍລະນີສ່ວນໃຫ່ຍ, ການໂຈມຕີແບບ DoS ມັກເກີດຂຶ້ນເພື່ອສ້າງຄວາມສູນເສຍດ້ານປະສິດທິພາບການ ຜະລິດ ແລະ ການເງິນຂອງອົງກອນ ຫຼື ເພື່ອດຶງດູດຄວາມສົນໃຈຂອງສາທາລະນະຊົນກ່ຽວກັບສາເຫດບາງປະການ. ຕົວຢ່າງຂອງກິດ ຈະກຳນີ້ແມ່ນໄດ້ອະທິບາຍໄວ້ໃນຄຳແນະນຳຂອງ ASD ທີ່ວ່າ *ຜູ້ມີສ່ວນກ່ຽວຂ້ອງກັບສາທາລະນະລັດ ປະຊາຊົນຈີນບຸກລຸກເຣົາເຕ ແລະ ອຸປະກອນ IoT ເພື່ອປະຕິບັດການບ໊ອດເນັດ*.

ເນື່ອງຈາກເສດຖະກິດຂອງພວກເຮົາມີການພັດທະນາເປັນດິຈິຕອນຫຼາຍຂຶ້ນ ແລະ ຈຳນວນອຸປະກອນ IoT ທີ່ຮັກສາຄວາມປອດໄພບໍ່ດີທີ່ເຊື່ອມຕໍ່ກັບອິນເຕີເນັດເພີ່ມຫຼາຍຂຶ້ນ, ການໂຈມຕີແບບ DoS ມີແນວໂນ້ມທີ່ຈະເພີ່ມຂຶ້ນຢ່າງຕໍ່ເນື່ອງ.

ເພື່ອຂັດຂວາງ ຫຼື ຫຼຸດປະສິດທິພາບຂອງບໍລິການອອນລາຍຂອງອົງກອນ, ຜູ້ບໍ່ປະສົງດີຈະໃຊ້ວິທີການຕ່າງໆ ດັ່ງຕໍ່ໄປນີ້:

- ການກຳນົດທິດທາງປະລິມານການຮັບສົ່ງຂໍ້ມູນເຄືອຂ່າຍທີ່ບໍ່ຕ້ອງການຈຳນວນຫຼາຍໄປຍັງບໍລິການອອນລາຍ ເພື່ອພະຍາຍາມທີ່ຈະບໍລິໂພກແບນວິດເຄືອຂ່າຍທີ່ມີຢູ່ທັງໝົດ
- ການກຳນົດທິດທາງການຮັບສົ່ງຂໍ້ມູນເຄືອຂ່າຍທີ່ເໝາະສົມໄປຍັງບໍລິການອອນລາຍເພື່ອພະຍາຍາມໃຊ້ຊັບພະຍາກອນການປະມວນຜົນຂອງຄອມພິວເຕີ
- ການນຳໃຊ້ຄອມພິວເຕີຫຼາຍເຄື່ອງ, ອຸປະກອນ IoT ຫຼື ອຸປະກອນເຊື່ອມຕໍ່ອິນເຕີເນັດອື່ນໆ ເພື່ອກຳນົດເສັ້ນທາງການຮັບສົ່ງຂໍ້ມູນເຄືອຂ່າຍໄປຍັງບໍລິການອອນລາຍຈາກຫຼາຍທິດທາງ ແລະ ໃນລະດັບທີ່ໃຫຍ່ກວ່າ, ການໂຈມຕີ DoS ປະເພດທົ່ວໄປເອີ້ນວ່າການໂຈມຕີ DoS ແບບກະຈາຍ (DDoS).
- ການແຮັກການລົງທະບຽນໂດເມນ ຫຼື ເຊີບເວີ DNS ຂອງອົງກອນເພື່ອພະຍາຍາມທີ່ຈະປ່ຽນເສັ້ນທາງຜູ້ໃຊ້ທີ່ຖືກຕ້ອງຕາມກົດໝາຍອອກຈາກການບໍລິການອອນລາຍຂອງອົງກອນ.

ອົງກອນບໍ່ສາມາດຫຼີກລ້ຽງການຕົກເປັນເປົ້າໝາຍຂອງການໂຈມຕີ DoS, ໄດ້ແຕ່ມີມາດຕະການຈຳນວນໜຶ່ງທີ່ອົງກອນສາມາດນຳໄປປະຕິບັດເພື່ອກຽມພ້ອມ ແລະ ຫຼຸດຜ່ອນຜົນກະທົບທີ່ອາດເກີດຂຶ້ນໄດ້. ການກະກຽມສຳລັບການໂຈມຕີ DoS ກ່ອນທີ່ຈະເກີດຂຶ້ນແມ່ນຍຸດທະສາດທີ່ດີທີ່ສຸດ, ເພາະບໍ່ໄດ້ກຽມຕົວໄວ້, ການຕອບສະໜອງຕໍ່ການໂຈມຕີ DoS ຈະເຮັດໄດ້ຍາກ ແລະ ມີປະສິດທິພາບໜ້ອຍລົງ.

ເຖິງແມ່ນວ່າອົງກອນຕ່າງໆ ຈະສຸມໃສ່ການປົກປ້ອງຕົນເອງຈາກການໂຈມຕີ DoS ເປັນຫຼັກ, ແຕ່ພວກເຂົາກໍ່ຄວນດຳເນີນຂັ້ນຕອນເພື່ອປ້ອງກັນບໍ່ໃຫ້ບໍລິການທາງອອນລາຍ ແລະ ອຸປະກອນທີ່ເຊື່ອມຕໍ່ອິນເຕີເນັດຖືກນຳໄປໃຊ້ໃນທາງທີ່ຜິດໂດຍຜູ້ບໍ່ປະສົງດີເພື່ອໂຈມຕີບຸກຄົນອື່ນ.

ການກຽມພ້ອມສຳລັບການໂຈມຕີ DoS

ໃນບໍລິບົດຂອງປະລິມານການໂຈມຕີ DoS ທີ່ເພີ່ມຫຼາຍຂຶ້ນໃນທົ່ວພາກພື້ນຂອງພວກເຮົາ, ກ່ອນທີ່ຈະດຳເນີນການໃດໆ ເພື່ອກະກຽມສຳລັບການໂຈມຕີ DoS, ອົງກອນຂອງທ່ານຄວນປະເມີນຄວາມຕ້ອງການທາງທຸລະກິດເພື່ອພິຈາລະນາວ່າບໍລິການອອນລາຍແຕ່ລະຢ່າງຂອງທ່ານຈະຕ້ອງຍັງຄົງເຮັດວຽກຢູ່ລະຫວ່າງການໂຈມຕີ DoS ຫຼື ບໍ່ ຫຼື ຢຸດການໃຫ້ບໍລິການຊົ່ວຄາວເປັນທີ່ຍອມຮັບໄດ້ຫຼືບໍ່.

ຖ້າອົງກອນຂອງທ່ານຕ້ອງການເພີ່ມຄວາມສາມາດໃນການທົນຕໍ່ການໂຈມຕີ DoS, ທ່ານຄວນປະຕິບັດມາດຕະການຕໍ່ໄປນີ້ຢ່າງຕັ້ງໜ້າ, ຖ້າເໝາະສົມ ແລະ ເປັນໄປໄດ້, ກ່ອນທີ່ຈະມີການໂຈມຕີ DoS.

- ຖ້າອົງກອນຂອງທ່ານໃຊ້ເຄືອຂ່າຍການຈັດສົ່ງເນື້ອຫາ (CDN), ທ່ານຄວນໃຊ້ມາດຕະການເພີ່ມເຕີມຕໍ່ໄປນີ້, ຕາມຄວາມເໝາະສົມ ແລະ ເປັນໄປໄດ້.
  - ພິຈາລະນານຳໃຊ້ CDN ທີ່ມີຟັງຊັນການເຮັດວຽກໃນອຸປະກອນປົກປ້ອງເຊີບເວີເວັບໄຊຕົ້ນກຳເນີດຂອງທ່ານຈາກການໂຈມຕີຂອງແອັບພລິເຄຊັນຕ່າງໆ ແລະ ຊັ້ນເຄືອຂ່າຍທີ່ຫຼາກຫຼາຍ - CDNs ບາງຕົວອາດຈະປະກອບມີຄຸນສົມບັດເຫຼົ່ານີ້ເປັນສ່ວນໜຶ່ງຂອງໄຟວໍແອັບພລິເຄຊັນເວັບທີ່ຂອບເຄືອຂ່າຍ.
  - ຫຼີກເວັ້ນການເປີດເຜີຍທີ່ຢູ່ IP (Internet Protocol) ຂອງເວັບເຊີບເວີຕົ້ນກຳເນີດຂອງທ່ານຕໍ່ສາທາລະນະໂດຍບໍ່ຈຳເປັນ ແລະ ກວດສອບໃຫ້ແນ່ໃຈວ່າການເປີດເຜີຍສາທາລະນະໃດໆໄດ້ຮັບການປົກປ້ອງຈາກການໂຈມຕີ DoS.
  - ຫຼີກເວັ້ນການນຳໃຊ້ທີ່ຢູ່ IP ສຳລັບເວັບເຊີບເວີຕົ້ນກຳເນີດຂອງທ່ານຜູ້ທີ່ບໍ່ປະສົງດີສາມາດຄາດເດົາໄດ້, ເຊັ່ນ: ທີ່ຢູ່ IP ຢູ່ໃນເຄືອຂ່າຍຍ່ອຍຂອງເຄືອຂ່າຍດຽວກັນຂອງທີ່ຢູ່ IP ທີ່ເປີດເຜີຍຕໍ່ສາທາລະນະຂອງການບໍລິການທາງອອນລາຍ.
  - ໃຊ້ການຄວບຄຸມການເຂົ້າເຖິງເຄືອຂ່າຍ (ເຊັ່ນ: ໄຟວໍ) ເພື່ອໃຫ້ແນ່ໃຈວ່າສະເພາະ CDN ແລະ ເຄືອຂ່າຍການຄຸ້ມຄອງທີ່ໄດ້ຮັບອະນຸຍາດຈາກອົງກອນຂອງທ່ານເທົ່ານັ້ນທີ່ສາມາດເຂົ້າເຖິງເວັບເຊີບເວີຕົ້ນກຳເນີດຂອງທ່ານໄດ້.
  - ພິຈາລະນານຳໃຊ້ການເຊື່ອມຕໍ່ເຄືອຂ່າຍທີ່ມີຄວາມຫຼາກຫຼາຍ ແລະ ຍືດຍຸນ, ເຊິ່ງອາດຈະປະກອບມີການເຊື່ອມຕໍ່ເຄືອຂ່າຍສ່ວນຕົວ, ລະຫວ່າງເວັບເຊີບເວີຕົ້ນກຳເນີດຂອງທ່ານ ແລະ ຜູ້ໃຫ້ບໍລິການ CDN ຂອງທ່ານ, ຖ້າທ່ານຕ້ອງການການປົກປ້ອງໃນລະດັບສູງສຳລັບເວັບເຊີບເວີຕົ້ນກຳເນີດຂອງທ່ານ.
  - ກຳນົດຄ່າ CDN, ເຊີບເວີເວັບຕົ້ນກຳເນີດ ແລະ ສ່ວນຫົວ HTTP ຂອງລູກຂ່າຍເພື່ອເພີ່ມປະສິດທິພາບປະລິມານການເກັບຂໍ້ມູນທີ່ດຳເນີນການ.
  - ພິຈາລະນາການແບ່ງສ່ວນຂອງເຊີບເວີເວັບຕົ້ນກຳເນີດເພື່ອໃຫ້ການຮ້ອງຂໍຈາກທີ່ຢູ່ IP ທີ່ມີຄວາມສ່ຽງຕ່ຳຈະຖືກຈັດການແຍກຕ່າງຫາກຕໍ່ການຮ້ອງຂໍຈາກທີ່ຢູ່ IP ທີ່ມີຄວາມສ່ຽງສູງ, ຖ້າທ່ານຕ້ອງການລະດັບຄວາມພ້ອມທີ່ສູງຂຶ້ນ.

- ພິຈາລະນາວ່າຟັງຊັ່ນການເຮັດວຽກ ແລະ ຄຸນນະພາບຂອງການບໍລິການທີ່ຍອມຮັບໄດ້ສຳລັບຜູ້ໃຊ້ທີ່ຖືກຕ້ອງຕາມກົດໝາຍຂອງການບໍລິການອອນລາຍ, ວິທີການຮັກສາຟັງຊັ່ນນັ້ນ ແລະ ຟັງຊັ່ນການເຮັດວຽກໃດທີ່ບໍ່ຈຳເປັນໃນລະຫວ່າງການໂຈມຕີ DoS.
- ຈັດຫາ ແລະ ໃຊ້ບໍລິການຫຼຸດຜ່ອນການໂຈມຕີ DoS ໃນຄລາວ.
- ພິຈາລະນາຫຼຸດພື້ນທີ່ການໂຈມຕີຂອງອົງກອນຂອງທ່ານໂດຍ:
  - ການອອກແຫຼ່ງການບໍລິການອອນລາຍພື້ນຖານ (ເຊັ່ນ: DNS) ໃຫ້ກັບຜູ້ໃຫ້ບໍລິການທີ່ມີຊື່ສຽງຜູ້ທີ່ສາມາດທົນຕໍ່ການໂຈມຕີ DoS ໄດ້.
  - ການແບ່ງສ່ວນການບໍລິການອອນລາຍທີ່ສຳຄັນ (ເຊັ່ນ: ອີເມວ) ອອກຈາກບໍລິການທາງອອນລາຍອື່ນໆທີ່ມີແນວໂນ້ມວ່າຈະຖືກກຳນົດເປົ້າໝາຍ (ເຊັ່ນ: ເວັບໄຊທ໌)
  - ເພື່ອໃຫ້ແນ່ໃຈວ່າການບໍລິການຫຼຸດຜ່ອນການໂຈມຕີ DoS ອະນຸຍາດສະເພາະການຮັບສົ່ງຂໍ້ມູນເຄືອຂ່າຍທີ່ກ່ຽວຂ້ອງກັບພອດເຄືອຂ່າຍຂອງບໍລິການອອນລາຍເທົ່ານັ້ນ.
- ສົນທະນາກັບຜູ້ໃຫ້ບໍລິການຂອງທ່ານກ່ຽວກັບລາຍລະອຽດຂອງຍຸດທະສາດການປ້ອງກັນ ແລະ ຫຼຸດຜ່ອນການໂຈມຕີ DoS, ໂດຍສະເພາະ:
  - ຄວາມສາມາດພິສູດທີ່ຈະທົນທານຕໍ່ການໂຈມຕີ DoS ຈາກທົ່ວໂລກ
  - ສະແດງໃຫ້ເຫັນປະຫວັດຂອງການຈັດການທັງການໂຈມຕີ DoS ແລະ ການທົດສອບການໂຈມຕີ DoS ທີ່ໄດ້ຮັບອະນຸຍາດທີ່ສົມບູນແບບ
  - ຄວາມສາມາດທີ່ຈະຫຼຸດຜ່ອນການໂຈມຕີ DoS ໂດຍອັດຕະໂນມັດເກືອບທຸກປະເພດໂດຍບໍ່ຕ້ອງມີມະນຸດເຂົ້າມາກ່ຽວຂ້ອງ, ເຊັ່ນ: ການວິເຄາະປະລິມານການຮັບສົ່ງຂໍ້ມູນໃນເຄືອຂ່າຍດ້ວຍຕົນເອງ
  - ວິທີການກຳນົດລາຄາການບໍລິການຂອງພວກເຂົາ ເຊັ່ນ: ຄ່າໃຊ້ຈ່າຍແມ່ນຄົງທີ່ ຫຼື ແບບຜັນແປຂຶ້ນຢູ່ກັບປະລິມານການຮັບສົ່ງຂໍ້ມູນໃນເຄືອຂ່າຍ ແລະ ແຫຼ່ງຂໍ້ມູນການປະມວນຜົນຄອມພິວເຕີທີ່ໃຊ້ ແລະ ທ່ານສາມາດກຳນົດຂີດຈຳກັດການຮຽກເກັບເງິນໄດ້ຫຼືບໍ່.
  - ເກນສຳລັບການແຈ້ງເຕືອນທ່ານ ຫຼື ປິດການບໍລິການອອນລາຍລະຫວ່າງການໂຈມຕີ DoS
  - ການດຳເນີນການທີ່ໄດ້ຮັບການອະນຸມັດລ່ວງໜ້າທີ່ສາມາດດຳເນີນການໄດ້ໃນລະຫວ່າງການໂຈມຕີ DoS
  - ຂໍ້ຕົກລົງການປ້ອງກັນການໂຈມຕີ DoS ກັບຜູ້ໃຫ້ບໍລິການຕົ້ນສະບັບ.
- ປະຕິບັດມາດຕະການເພື່ອກວດຫາການໂຈມຕີ DoS ເຊັ່ນ: ການຕິດຕາມເວລາຈິງ ແລະ ການແຈ້ງເຕືອນຄວາມພ້ອມຂອງລະບົບ, ປະລິມານການໃຊ້ງານເຄືອຂ່າຍ, ຊັບພະຍາກອນປະມວນຄອມພິວເຕີ ແລະ ຄ່າໃຊ້ຈ່າຍທີ່ກ່ຽວຂ້ອງ.
- ກະກຽມເວຊັນຄົງທີ່ຂອງເວັບໄຊທ໌ຂອງທ່ານທີ່ຕ້ອງການປະມວນຜົນ ແລະ ແບນວິດຂັ້ນຕ່ຳ ເພື່ອອຳນວຍຄວາມສະດວກໃນການບໍລິການຢ່າງຕໍ່ເນື່ອງໃນລະຫວ່າງການໂຈມຕີ DoS.
- ຈັດຫາ ແລະ ໃຊ້ບໍລິການອອນລາຍທີ່ມີຄວາມຢືດຢຸ່ນສູງດ້ວຍແບນວິດຂະໜາດໃຫຍ່, ຊັບພະຍາກອນການປະມວນຜົນຄອມພິວເຕີທີ່ພຽງພໍ, ສະຖານທີ່ໂຮດທີ່ກະແຈກກະຈາຍຕາມພູມສັນຖານ ແລະ ການລ້າງຂໍ້ມູນການຮັບສົ່ງຂໍ້ມູນໃນຄລາວ ເພື່ອລຶບຂໍ້ມູນເຄືອຂ່າຍທີ່ບໍ່ຕ້ອງການ – ເຊິ່ງໂດຍທົ່ວໄປແລ້ວລວມມີການໃຊ້ CDN ທີ່ມີຊື່ສຽງ ເພື່ອຈັດເກັບເນື້ອຫາເວັບໄຊທ໌ຄົງທີ່ ແລະ ປົກປ້ອງເຊີບເວີເວັບຕົ້ນກຳເນີດຂອງທ່ານຈາກຂໍ້ມູນການຮັບສົ່ງຂໍ້ມູນເຄືອຂ່າຍທີ່ບໍ່ຕ້ອງການ.
- ປົກປ້ອງຊື່ໂດເມນຂອງອົງກອນຂອງທ່ານໂດຍໃຊ້ການລັອກຜູ້ໃຫ້ບໍລິການລົງທະບຽນ, ຢືນຢັນລາຍລະອຽດການຕິດຕໍ່ການລົງທະບຽນໂດເມນ ແລະ ລາຍລະອຽດອື່ນໆທີ່ຖືກຕ້ອງ ແລະ ປະຕິບັດຕາມຄຳແນະນຳເພີ່ມເຕີມທີ່ລະບຸໄວ້ໃນເອກະສານເຜີຍແຜ່ *ການຮັກສາຄວາມປອດໄພລະບົບຊື່ໂດເມນສຳລັບເຈົ້າຂອງໂດເມນ* ຂອງ ASD.
- ຮັກສາຂໍ້ມູນຕິດຕໍ່ຫຼ້າສຸດສຳລັບຜູ້ໃຫ້ບໍລິການຂອງທ່ານ ແລະ ແບ່ງປັນລາຍລະອຽດການຕິດຕໍ່ຂອງອົງກອນຂອງທ່ານກັບພວກເຂົາ, ກວດສອບໃຫ້ແນ່ໃຈວ່າການຕິດຕໍ່ທັງໝົດແມ່ນພ້ອມໃຫ້ບໍລິການຕາມຄວາມຕ້ອງການຂອງອົງກອນຂອງທ່ານ ເຊັ່ນ: ຕະຫຼອດ 24 ຊົ່ວໂມງ, 7 ວັນຕໍ່ອາທິດ.
- ໃຫ້ລາຍລະອຽດການຕິດຕໍ່ນອກວົງການຂອງອົງການຂອງທ່ານສຳລັບຊ່ອງທາງການສື່ສານທີ່ເຊື່ອຖືໄດ້ໃຫ້ກັບຜູ້ໃຫ້ບໍລິການຂອງທ່ານ, ເມື່ອຊ່ອງທາງການສື່ສານປົກກະຕິລົ້ມເຫຼວ.
- ພັດທະນາ, ນຳໄປປະຕິບັດ ແລະ ດູແລຮັກສາແຜນການຕອບສະໜອງເຫດການດ້ານຄວາມປອດໄພທາງໄຊເບີ, ໂດຍຄວບຄຸມເຖິງການໂຈມຕີ DoS ຫຼາຍປະເພດຕໍ່ບໍລິການອອນລາຍຂອງທ່ານແຕ່ລະປະເພດທີ່ຈຳເປັນເພື່ອຕ້ານກັບການໂຈມຕີ DoS ແລະ ໃຊ້ແຜນການດັ່ງກ່າວຢ່າງໜ້ອຍປີລະຄັ້ງ.
- ແອັບພລິເຄຊັນສະຖາປັດຕະຍະກຳເພື່ອປົກປ້ອງການຟັງຊັ່ນການທຳງານທີ່ມັກຖືກລະເມີດທີ່ໃຊ້ຊັບພະຍາກອນການປະມວນຜົນຄອມພິວເຕີເພີ່ມຂຶ້ນ ຫຼື ເຮັດໃຫ້ເກີດຄ່າໃຊ້ຈ່າຍທາງດ້ານການເງິນເພີ່ມເຕີມ (ເຊັ່ນ: ການສົ່ງຂໍ້ຄວາມ SMS).
  - ການປົກປ້ອງລວມມີການຈຳກັດອັດຕາ ແລະ ການຢືນຢັນວ່າຄຳຮ້ອງຂໍແມ່ນມາຈາກມະນຸດ.

- ດຳເນີນການທົດສອບການໂຈມຕີ DoS ລວມທັງການກຳນົດເປົ້າໝາຍການໄຫຼຂອງເຫດຜົນທີ່ບໍ່ເໝາະສົມໃນການເຮັດວຽກຂອງແອັບພລິເຄຊັນ.
- ດຳເນີນການທົດສອບການໂຫຼດທີ່ກວ້າງຂຶ້ນເພື່ອກຳນົດ ແລະ ແກ້ໄຂສູດຄິດໄລ່ DoS.

ຕອບສະໜອງຕໍ່ການໂຈມຕີ DoS

ຖ້າອົງກອນຂອງທ່ານບໍ່ໄດ້ກຽມພ້ອມຮັບມືກັບການໂຈມຕີ DoS, ທ່ານສາມາດພະຍາຍາມປະຕິບັດບາງມາດຕະການຂ້າງເທິງໃນລະຫວ່າງການໂຈມຕີ DoS, ເຖິງແມ່ນວ່າມາດຕະການເຫຼົ່ານີ້ຈະມີປະສິດທິພາບໜ້ອຍ ແລະ ຕ້ອງໃຊ້ເວລາໃນການປະຕິບັດ, ສົ່ງຜົນໃຫ້ຄວາມສາມາດໃນການຕອບສະໜອງຂອງອົງກອນຫຼຸດລົງ.

ອົງກອນຂອງທ່ານຄວນນຳມາດຕະການດັ່ງຕໍ່ໄປນີ້ມາໃຊ້ໃນລະຫວ່າງການໂຈມຕີ DoS, ຕາມຄວາມເໝາະສົມ ແລະ ເປັນໄປໄດ້.

- ບັງຄັບໃຊ້ແຜນການຕອບສະໜອງຕໍ່ເຫດການດ້ານຄວາມປອດໄພທາງໄຊເບີຂອງທ່ານ.
- ສອບຖາມຜູ້ໃຫ້ບໍລິການຂອງທ່ານວ່າພວກເຂົາສາມາດປະຕິບັດການຕອບສະໜອງໄດ້ທັນທີຫຼືບໍ່ - ຖ້າທ່ານຍັງບໍ່ໄດ້ປຶກສາຫາລືກ່ຽວກັບຄວາມສາມາດໃນການຕອບສະໜອງຂອງພວກເຂົາ, ທ່ານອາດຈະພົບວ່າພວກເຂົາບໍ່ສາມາດ ຫຼື ບໍ່ເຕັມໃຈທີ່ຈະຕອບສະໜອງ ຫຼື ຄິດຄ່າທຳນຽມເພີ່ມເຕີມ.
- ປິດໃຊ້ງານຟັງຊັນທີ່ບໍ່ສຳຄັນ ຫຼື ລຶບເນື້ອຫາທີ່ບໍ່ສຳຄັນອອກຈາກການບໍລິການອອນລາຍຂອງທ່ານທີ່ເຮັດໃຫ້ການໂຈມຕີ DoS ໃນປະຈຸບັນມີປະສິດທິພາບ, ຕົວຢ່າງ, ນຳໃຊ້ເວັບໄຊທ໌ເວີຊັນທີ່ບໍ່ມີຟັງຊັນການຄົ້ນຫາ, ເນື້ອຫາແບບເຄື່ອນໄຫວ ຫຼື ໄຟລ໌ຂະໜາດໃຫຍ່.
- ຮັກສາການສື່ສານກັບລູກຄ້າ ແລະ ຜູ້ໃຫ້ບໍລິການຂອງທ່ານ, ລວມທັງຜູ້ໃຫ້ບໍລິການຫຼຸດຜ່ອນການໂຈມຕີ DoS, ແລະ ກວດສອບຄວາມພ້ອມໃຊ້ງານຂອງບໍລິການອອນລາຍຂອງທ່ານຢ່າງຕໍ່ເນື່ອງ.
- ຄວນພິຈາລະນາປ່ຽນທີ່ຢູ່ IP ຂອງເວັບເຊີບເວີຕົ້ນກຳເນີດຂອງທ່ານ ຖ້າຖືກກຳນົດເປົ້າໝາຍໂດຍກົງ ແລະ ຫຼີກເວັ້ນການເປີດເຜີຍທີ່ຢູ່ IP ໃໝ່ຕໍ່ສາທາລະນະໂດຍບໍ່ມີການປ້ອງກັນໃດໆທັງໝົດ.
- ລາຍງານການໂຈມຕີ DoS ກັບພາກສ່ວນທີ່ກ່ຽວຂ້ອງ ລວມທັງ ASD ແລະ NCSC-NZ ຕາມພາກສ່ວນ ‘ລາຍລະອຽດການຕິດຕໍ່’ ຂອງເອກະສານເຜີຍແຜ່.

ຫຼີກເວັ້ນການສະໜັບສະໜູນໃນການໂຈມຕີ DoS

ອົງກອນຂອງທ່ານຄວນນຳມາດຕະການຕໍ່ໄປນີ້ມາໃຊ້ ເພື່ອຫຼີກເວັ້ນການມີສ່ວນຮ່ວມໃນການໂຈມຕີ DoS ໂດຍບໍ່ຕັ້ງໃຈ ທີ່ອາດຈະສົ່ງຜົນກະທົບຕໍ່ຄົນອື່ນໄດ້.

- ຫຼີກເວັ້ນການເປີດເຜີຍການບໍລິການ, ອຸປະກອນ IoT ແລະ ອຸປະກອນອື່ນໆ ທີ່ເຊື່ອມຕໍ່ອິນເຕີເນັດກັບອິນເຕີເນັດທີ່ບໍ່ຈຳເປັນ, ການຕັ້ງຄ່າທີ່ບໍ່ປອດໄພ ຫຼື ມີການບຳລຸງຮັກສາບໍ່ພຽງພໍ.
- ກຳນົດຄ່າ, ດູແລຮັກສາ ແລະ ກວດສອບການບໍລິການ, ອຸປະກອນ IoT ແລະ ອຸປະກອນອື່ນໆ ທີ່ເຊື່ອມຕໍ່ອິນເຕີເນັດຢ່າງປອດໄພ.
  - ການແນະນຳເພີ່ມເຕີມສຳລັບທຸລະກິດຂະໜາດນ້ອຍແມ່ນມີຢູ່ໃນເອກະສານເຜີຍແຜ່ *ອຸປະກອນອິນເຕີເນັດຂອງສິ່ງຕ່າງໆ* ແລະ *ຮັກສາຄວາມປອດໄພ Wi-Fi ແລະ ເຣົາເຕີຂອງທ່ານ* ຂອງ ASD.

ຖ້າອົງກອນຂອງທ່ານກຳລັງດຳເນີນການບໍລິການອອນລາຍ, ທ່ານຄວນໃຊ້ມາດຕະການເພີ່ມເຕີມຕໍ່ໄປນີ້.

- ໃຫ້ຄວາມສຳຄັນກັບການກວດສອບໂປໂຕຄອນທີ່ລະບຸໄວ້ໃນຄຳແນະນຳ *ການໂຈມຕີການຂະຫຍາຍສັນຍານໂດຍໃຊ້ UDP* ຂອງໜ່ວຍງານຄວາມໝັ້ນຄົງທາງໄຊເບີ ແລະ ໂຄງສ້າງພື້ນຖານຄວາມປອດໄພຂອງສະຫະລັດອາເມລິກາ (CISA).
- ກວດສອບສູດຄິດໄລ່ຂະຫຍາຍໃໝ່ເມື່ອມີການລະບຸ ແລະ ຮັກສາຄວາມປອດໄພບໍລິການອອນລາຍຂອງທ່ານຈາກສູດຄິດໄລ່ເຫຼົ່ານັ້ນ.
- ກຳນົດຄ່າການຄວບຄຸມການເຂົ້າເຖິງເຄືອຂ່າຍທັງຂາເຂົ້າ ແລະ ຂາອອກ ເພື່ອຈຳກັດການເຂົ້າເຖິງການບໍລິການ ແລະ ອົງກອນທີ່ໄດ້ຮັບອະນຸຍາດ.

- ບລັອກການເຂົ້າເຖິງສາທາລະນະທີ່ບໍ່ເປີດເຜີຍຊື່ ສຳລັບການບໍລິການອອນລາຍທີ່ມີແນວໂນ້ມຈະຂະຫຍາຍສັນຍານຖ້າບໍ່ຈຳເປັນ.
- ພິຈາລະນາໃຊ້ກົນໄກການຈຳກັດອັດຕາ ເພື່ອຫຼຸດຜ່ອນຜົນທີ່ຕາມມາຈາກການລ່ວງລະເມີດ, ຖ້າການບລັອກ ຫຼື ນຳໃຊ້ການຄວບຄຸມການເຂົ້າເຖິງເປັນໄປໄດ້ ຫຼື ບໍ່ເໝາະສົມ.

ຂໍ້ມູນເພີ່ມເຕີມ

ຄູ່ມືຄວາມປອດໄພຂອງຂໍ້ມູນ ຂອງ ASD ແມ່ນກອບຄວາມປອດໄພທາງໄຊເບີທີ່ອົງກອນຕ່າງໆສາມາດນຳໄປໃຊ້ເພື່ອປົກປ້ອງລະບົບ ແລະ ຂໍ້ມູນຂອງຕົນຈາກໄພຂົ່ມຂູ່ທາງໄຊເບີ. ຄຳແນະນຳໃນ *ຍຸດທະສາດເພື່ອຫຼຸດຜ່ອນເຫດການຄວາມປອດໄພທາງໄຊເບ*, ຄວບຄູ່ໄປກັບ*ສິ່ງສຳຄັນທັງແປດປະການ*, ແມ່ນເປັນການເສີມສ້າງກອບວຽກນີ້.

ຄູ່ມືການຮັກສາຄວາມປອດໄພຂໍ້ມູນຂ່າວສານນິວຊີແລນ ແມ່ນຄູ່ມືຂອງລັດຖະບານນິວຊີແລນກ່ຽວກັບການຮັບປະກັນຂໍ້ມູນ ແລະ ຄວາມປອດໄພຂອງລະບົບຂໍ້ມູນ. ເປັນຄູ່ມືສຳລັບຜູ້ປະຕິບັດງານທີ່ອອກແບບມາເພື່ອຕອບສະໜອງຄວາມຕ້ອງການຂອງຜູ້ບໍລິຫານດ້ານຄວາມປອດໄພຂໍ້ມູນຂອງໜ່ວຍງານ ລວມທັງຜູ້ຂາຍ ຜູ້ຮັບເໝົາ ແລະ ທີ່ປຶກສາທີ່ໃຫ້ບໍລິການແກ່ໜ່ວຍງານ.

ຂໍ້ມູນເພີ່ມເຕີມກ່ຽວກັບປະເພດການໂຈມຕີ DoS ຕ່າງໆແມ່ນມີຢູ່ໃນເອກະສານເຜີຍແຜ່ *ຄູ່ມືດ່ວນ DDoS* ແລະ *ຄວາມເຂົ້າໃຈ ແລະ ຕອບໂຕ້ຕໍ່ການໂຈມຕີປະຕິເສດການບໍລິການທີ່ແຈກຢາຍ*.

ຂໍ້ມູນການຕິດຕໍ່

ໃນປະເທດອົດສະຕາລີ, ຖ້າທ່ານມີຄຳຖາມໃດໆກ່ຽວກັບຄຳແນະນຳນີ້ ຂຽນເຖິງ ASD ຫຼື ໂທຫາ 1300 CYBER1 (1300 292 371).

ໃນປະເທດນິວຊີແລນ, ຖ້າຕ້ອງການລາຍງານເຫດການທີ່ກ່ຽວຂ້ອງກັບຄວາມປອດໄພທາງໄຊເບີໃຫ້ສົ່ງອີເມວໄປທີ່ incidents@ncsc.govt.nz ຫຼື ເຂົ້າໄປທີ່ໜ້າເວັບ ລາຍງານເຫດການ ຂອງ NCSC-NZ.

ການປະຕິເສດຄວາມຮັບຜິດຊອບ

ເນື້ອຫາໃນຄູ່ມືນີ້ແມ່ນມີລັກສະນະທົ່ວໄປ ແລະ ບໍ່ຄວນຖືເປັນຄຳແນະນຳທາງດ້ານກົດໝາຍ ຫຼື ໃຊ້ເປັນຂໍ້ມູນຊ່ວຍເຫຼືອໃນສະຖານະການສະເພາະໃດໜຶ່ງ ຫຼື ສະຖານະການສຸກເສີນ. ໃນເລື່ອງທີ່ສຳຄັນໃດໆ, ທ່ານຄວນຊອກຫາຄຳແນະນຳຈາກຜູ້ຊ່ຽວຊານອິດສະຫຼະທີ່ເໝາະສົມກັບສະຖານະການຂອງທ່ານເອງ.

ເຄື່ອງຈັກພາບຈະບໍ່ຮັບຜິດຊອບໃດໆ ຕໍ່ຄວາມເສຍຫາຍ, ການສູນເສຍ ຫຼື ຄ່າໃຊ້ຈ່າຍໃດໆທີ່ເກີດຂຶ້ນອັນເປັນຜົນມາຈາກເພິ່ງພາຂໍ້ມູນທີ່ມີຢູ່ໃນຄູ່ມືນີ້.

ລິຂະສິດ

ການນຳໃຊ້ກາເຄື່ອງໝາຍ

ຖ້າຕ້ອງການຂໍ້ມູນເພີ່ມເຕີມ ຫຼື ລາຍງານເຫດການຄວາມປອດໄພທາງໄຊເບີ, ໃຫ້ຕິດຕໍ່ພວກເຮົາ:

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

ເບີໂທນີ້ສາມາດໃຊ້ໄດ້ພາຍໃນອອສເຕຣເລັຍເທົ່ານັ້ນ.

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre