ສາທາລະນະລັດ ປະຊາທິປະໄຕ ປະຊາຊົນລາວ
ສັນຕິພາບ ເອກະລາດ ປະຊາທິປະໄຕ ເອກະພາບ ວັດທະນະຖາວອນ

ກະຊວງເຕັກໂນໂລຊີ ແລະ ການສື່ສານ
ສູນອິນເຕີເນັດ ແຫ່ງຊາດ

ເລກທີ 076 /ສອຊ
ນະຄອນຫຼວງວຽງຈັນ, ວັນທີ 22 ມັງກອນ 2026

ກົດລະບຽບ

ວ່າດ້ວຍ ມາດຕະການຮັກສາຄວາມປອດໄພ ແລະ ການສຳຮອງຂໍ້ມູນ
ການບໍລິການລະບົບສູນຂໍ້ມູນຂອງ ສູນອິນເຕີເນັດ ແຫ່ງຊາດ

- ອີງຕາມ ຂໍ້ຕົກລົງວ່າດ້ວຍການຈັດຕັ້ງ ແລະ ການເຄື່ອນໄຫວ ຂອງສູນອິນເຕີເນັດ ແຫ່ງຊາດ, ສະບັບເລກທີ 193/ກຕສ, ລົງວັນທີ 02 ເດືອນກຸມພາ 2022.

ສູນອິນເຕີເນັດ ແຫ່ງຊາດ ຕໍ່ອັກສອນຫຍໍ້ "ສອຊ" ເປັນພາສາ ສາກົນ Lao National Internet Center ຂຽນຫຍໍ້ "LANIC" (ຕໍ່ໄປນີ້ເອີ້ນວ່າຜູ້ໃຫ້ບໍລິການ) ເປັນສູນໜຶ່ງທີ່ມີສະຖານະທຽບເທົ່າກົມ ໃນກົງຈັກການຈັດຕັ້ງ ຂອງ ກະຊວງເຕັກໂນໂລຊີ ແລະ ການສື່ສານ ຖືຄວາມສຳຄັນໃນການຄຸ້ມຄອງການຮັກສາຄວາມປອດໄພ ແລະ ການສຳຮອງຂໍ້ມູນ ຂອງບັນດາຂໍ້ມູນ ແລະ ລະບົບຕ່າງໆທີ່ຕິດຕັ້ງ ແລະ ຝາກໄວ້ຢູ່ ສອຊ ໃຫ້ມີຄວາມຮັບປະກັນ ສາມາດສະໜອງການໃຫ້ບໍລິການ ແລະ ການເຮັດວຽກຂອງລະບົບໄດ້ເປັນປົກກະຕິ ແກ່ບັນດາ ນິຕິບຸກຄົນ ແລະອີງການຈັດຕັ້ງ ທີ່ນຳໃຊ້ຊັບພະຍາກອນ ແລະ ບໍລິການຂອງ ສອຊ (ຕໍ່ໄປນີ້ເອີ້ນວ່າ ຜູ້ໃຊ້ບໍລິການ), ດັ່ງນັ້ນຈຶ່ງສ້າງກົດລະບຽບ ວ່າດ້ວຍ ມາດຕະການຮັກສາຄວາມປອດໄພ ແລະ ການສຳຮອງຂໍ້ມູນ ການບໍລິການຂອງ ສູນອິນເຕີເນັດ ແຫ່ງຊາດ ດັ່ງມີລາຍລະອຽດລຸ່ມນີ້:

ມາດຕາ 01: ຈຸດປະສົງ.

ລະບຽບສະບັບນີ້ ນຳໃຊ້ເປັນບ່ອນອີງເພື່ອກຳນົດຫຼັກການ, ລະບຽບການ ແລະ ມາດຕະການໃນການຄຸ້ມຄອງ ການຮັກສາຄວາມປອດໄພ ແລະ ການສຳຮອງຂໍ້ມູນຂອງລະບົບຕ່າງໆ ຂອງນິຕິບຸກຄົນ ແລະ ອົງການຈັດຕັ້ງ ທີ່ມາໃຊ້ຊັບພະຍາກອນ ແລະ ການບໍລິການຂອງ ສູນອິນເຕີເນັດ ແຫ່ງຊາດ.

ມາດຕາ 02: ຂອບເຂດການນຳໃຊ້.

ລະບຽບສະບັບນີ້ ນຳໃຊ້ສະເພາະນິຕິບຸກຄົນ ແລະ ອົງການຈັດຕັ້ງຕ່າງໆ ທີ່ມາໃຊ້ ການບໍລິການລະບົບສູນຂໍ້ມູນເປັນຕົ້ນ ລະບົບເຊົ່າພື້ນທີ່ຝາກຂໍ້ມູນເວັບໄຊ (Web Hosting), ລະບົບຄລາວໃຫ້ບໍລິການເຊີເວີຈຳລອງ (VPS), ເຊົ່າພື້ນທີ່ຫ້ອງເຄື່ອງຝາອຸປະກອນ (Co-location) ຂອງ ສູນອິນເຕີເນັດ ແຫ່ງຊາດ.

ມາດຕາ 03: ສິດ ແລະ ໜ້າທີ່ ຂອງຜູ້ໃຫ້ບໍລິການ.

1. ຄຸ້ມຄອງລະບົບການບໍລິການ, ບັນດາອຸປະກອນຕ່າງໆ ທີ່ຕິດຕັ້ງຢູ່ຫ້ອງເຄື່ອງ ຂອງ ສອຊ ໃຫ້ສາມາດເຮັດວຽກໄດ້ປົກກະຕິຕະຫຼອດ 24 ຊມ/7 ວັນ.
2. ກວດກາລະບົບທີ່ຜູ້ໃຊ້ບໍລິການມາຝາກ, ຖ້າພົບວ່າບໍ່ມີຄວາມປອດໄພສາມາດຢຸດໃຫ້ການບໍລິການ ແລະ ຮື້ຖອນອອກຈາກ ສອຊ.
3. ອຳນວຍຄວາມສະດວກ ແລະ ໃຫ້ຄວາມຊ່ວຍເຫຼືອທາງເຕັກນິກຕໍ່ຜູ້ໃຊ້ບໍລິການ.

4. ແຈ້ງເຕືອນຜູ້ໃຊ້ບໍລິການລ່ວງໜ້າ ເມື່ອມີການບຳລຸງຮັກສາຫ້ອງເຄື່ອງ ຫຼື ປັບປຸງລະບົບຕ່າງໆ.
5. ສອຊ ຈະບໍ່ຮັບຜິດຊອບຕໍ່ຄວາມເສຍຫາຍໃດໆ ຫຼື ການສູນເສຍຂໍ້ມູນ, ການຢຸດຊະງັກທາງທຸລະກິດ ຫຼື ຄວາມເສຍຫາຍອື່ນໆ ທີ່ເກີດຈາກອຸປະກອນ ຫຼື ລະບົບຂອງຜູ້ໃຊ້ບໍລິການເອງ.

ມາດຕາ 04: ສິດ ແລະ ໜ້າທີ່ ຂອງຜູ້ໃຊ້ບໍລິການ.

1. ຕ້ອງປະຕິບັດກົດລະບຽບສະບັບນີ້ຢ່າງເຂັ້ມງວດ.
2. ກວດກາ ແລະ ບຳລຸງຮັກສາບັນດາອຸປະກອນ ແລະ ລະບົບຕ່າງໆຂອງຕົນ ໃຫ້ມີຄວາມຮັບປະກັນໃນດ້ານຄວາມປອດໄພໃນການໃຊ້ງານ.
3. ຕ້ອງໃຊ້ລະຫັດຜ່ານທີ່ປອດໄພ ແລະ ປ່ຽນລະຫັດຢ່າງເປັນປະຈຳ.
4. ຮັກສາຂໍ້ມູນການເຂົ້າຫາລະບົບ (Username, Password) ໄວ້ເປັນຄວາມລັບ ແລະ ຮັບຜິດຊອບຕໍ່ການຮັກສາຄວາມປອດໄພຂອງໝາຍເລກໂອຜີ, ບັນດາຂໍ້ມູນເວັບໄຊ ທີ່ຕົນເປັນຜູ້ຄຸ້ມຄອງ.
5. ຮັບຜິດຊອບຕໍ່ທຸກການກະທຳທີ່ເກີດຂຶ້ນຈາກບັນດາອຸປະກອນ, ລະບົບ ແລະ ການໃຊ້ງານຂອງຕົນ ຮັບປະກັນໃຫ້ມີການນຳໃຊ້ໃນທາງທີ່ຖືກຕ້ອງຕາມລະບຽບການ, ລະບຽບກົດໝາຍຂອງ ສປປ ລາວ ແລະ ລະບຽບການອື່ນໆທີ່ກ່ຽວຂ້ອງ.
6. ຕ້ອງສຳຮອງຂໍ້ມູນຂອງຕົນເອງຢ່າງເປັນປະຈຳ ແລະ ແຍກເກັບຮັກສາໄວ້ຫຼາຍບ່ອນຕ່າງກັນ (ໃນລະບົບ, ນອກລະບົບ ແລະ ອື່ນໆ).
7. ຕ້ອງຮັບຜິດຊອບຕໍ່ຄວາມເສຍຫາຍຂອງລະບົບ, ການສູນເສຍຂໍ້ມູນ ແລະ ການຢຸດຊະງັກທາງທຸລະກິດ, ຫຼື ຄວາມເສຍຫາຍອື່ນໆ ທີ່ເກີດຈາກອຸປະກອນ ຫຼື ລະບົບພາຍໃນຂອງຜູ້ມາໃຊ້ບໍລິການເອງ.

ມາດຕາ 05: ການນຳໃຊ້ລະບົບປະຕິບັດການ (OS) ແລະ ຊອບແວ (Software).

1. ຜູ້ໃຊ້ບໍລິການສາມາດນຳໃຊ້ລະບົບປະຕິບັດການທີ່ມີ License ແລະ ລະບົບປະຕິບັດການທີ່ຜູ້ໃຫ້ບໍລິການຮອງຮັບເທົ່ານັ້ນ.
2. ຜູ້ໃຊ້ບໍລິການຕ້ອງຮັບປະກັນວ່າລະບົບປະຕິບັດການທີ່ນຳໃຊ້ໃນການຕິດຕັ້ງແມ່ນໄດ້ຮັບການລົງທະບຽນ (Activate License) ແລະ ສະໜັບສະໜຸນຈາກຜູ້ຜະລິດຢ່າງເປັນທາງການ ພ້ອມທັງໄດ້ຮັບການອັບເດດດ້ານຄວາມປອດໄພຢ່າງສະໝ່ຳສະເໝີ, ການຕິດຕັ້ງລະບົບປະຕິບັດການທີ່ດັດແປງ, ແຮັກ ຫຼື ແຄັຣກ ແມ່ນບໍ່ອະນຸຍາດໃຫ້ຕິດຕັ້ງຢ່າງເດັດຂາດ.
3. ຜູ້ໃຊ້ບໍລິການຕ້ອງຮັບປະກັນຊອຟແວທັງໝົດທີ່ຕິດຕັ້ງຢູ່ ເປັນຊອຟແວທີ່ຖືກຕ້ອງຕາມກົດໝາຍ ແລະ ມີໃບອະນຸຍາດທີ່ຖືກຕ້ອງ (Software License).
4. ການຕິດຕັ້ງຊອຟແວທີ່ມີຈຸດອ່ອນດ້ານຄວາມປອດໄພ ແລະ ບໍ່ໄດ້ຮັບການອັບເດດແມ່ນຖືວ່າເປັນການລະເມີດລະບຽບການນຳໃຊ້, ຕ້ອງມີການກວດກາຊ່ອງໂຫວ່ ແລະ ປັບປຸງ Update/Upgrade ຊອຟແວເປັນປະຈຳ ແລະ ທັນເວລາ.
5. ການນຳໃຊ້ ຊອຟແວແບບເປີດ (Open Sources) ຜູ້ໃຊ້ບໍລິການຕ້ອງຮັບຜິດຊອບຕໍ່ຄວາມສ່ຽງ ແລະ ຜົນກະທົບທີ່ອາດຈະເກີດຂຶ້ນຈາກລະບົບຂອງຕົນ.
6. ຕ້ອງກຳນົດການຕັ້ງຄ່າຊອຟແວເພື່ອໃຫ້ມີການອັບເດດໂດຍອັດຕະໂນມັດ.
7. ຖ້າທາງ ສອຊ ກວດພົບວ່າ ຊອຟແວໝົດອາຍຸ, ບໍ່ໄດ້ຮັບການພັດທະນາ ແລະ ຮັບແຈ້ງວ່າມີຈຸດອ່ອນດ້ານຄວາມປອດໄພ ຕ້ອງໄດ້ຮັບການອັບເກດ ຫຼື ຖືກຖອນການຕິດຕັ້ງທັນທີ.

ມາດຕາ 06: ອຸປະກອນ ແລະ ລະບົບທີ່ຖືກເກືອດຫ້າມ.

1. ຫ້າມໃຫ້ຕິດຕັ້ງ, ນຳໃຊ້ຊອບແວ ແລະ ດຳເນີນກິດຈະກຳດັ່ງຕໍ່ໄປນີ້:

- ຕິດຕັ້ງ, ເກັບຮັກສາ ຫຼື ແຈກຢາຍຊອຟແວເຖື່ອນ, ບັນດາເນື້ອຫາທີ່ຜິດລິຂະສິດ ຫຼື ຜິດລະບຽບກົດໝາຍ, ເນື້ອຫາລາມົກອາບາຈານ, ການພະນັນອອນລາຍ, ຢາເສບຕິດ, ຄ້າຂາຍເຖື່ອນ, ຫວຍເຖື່ອນ.
- ເຄື່ອງມື ແລະ ຊອຟແວຊອກຫາຈຸດອ່ອນໂດຍບໍ່ໄດ້ຮັບອະນຸຍາດ.
- ເຄື່ອງມື ແລະ ຊອຟແວທີ່ໃຊ້ດຳເນີນການໂຈມຕີ DDoS, ໂຈມຕີທາງໄຊເບີ ລວມເຖິງພຶດຕິກຳຕ່າງໆທີ່ສະແດງໃຫ້ເຫັນເປັນໄພຄຸກຄາມທາງໄຊເບີ.
- ເຄື່ອງມື ແລະ ຊອຟແວສຳຫຼັບຂຸດຄົ້ນຊັບສິນ ດິຈິຕອນ ເປັນຕົ້ນ: Bitcoin, Ethereum, Tether ໂດຍບໍ່ໄດ້ຮັບອານຸຍາດ.
- ເຄື່ອງມື ແລະ ຊອຟແວສຳລັບສ້າງ ຫຼື ແຈກຢາຍ Malware ຫຼື Virus
- ເຄື່ອງມື ແລະ ຊອຟແວສຳລັບແຮັກ ຫຼື ເຈາະລະບົບໂດຍບໍ່ໄດ້ຮັບອະນຸຍາດ.
- ລະບົບທີ່ເຮັດໃຫ້ເກີດໂປຣເຊດທີ່ໃຊ້ຊັບພະຍາກອນຫຼາຍເກີນໄປ (High Performance Processing) ແລະ ມີຜົນກະທົບຕໍ່ການບໍລິການອື່ນໆ.

2. ຫ້າມນຳໃຊ້, ແຈກຢາຍ Malware, ແບ່ງປັນຊອຟແວທີ່ລະເມີດໃບອະນຸຍາດ, ໂປຣແກຣມ ຫຼື Script ທີ່ເປັນອັນຕະລາຍ.
3. ຫ້າມດຳເນີນການໃດໆທີ່ມີພຶດຕິກຳໂຈມຕີໃນຮູບແບບ Phishing, DDoS, ການສະແກນຈຸດອ່ອນ, ຫຼື ພະຍາຍາມເຂົ້າເຖິງລະບົບໂດຍບໍ່ໄດ້ຮັບອະນຸຍາດເປັນຕົ້ນ.
4. ຫ້າມນຳສົ່ງອີເມວຂີ້ເຫຍື້ອ (spam) ຫຼື ການສົ່ງອີເມວຈຳນວນຫຼາຍໂດຍບໍ່ໄດ້ຮັບອະນຸຍາດ.

ມາດຕາ 07: ການກຳນົດດ້ານຄວາມປອດໄພ.

ກ. ຄວາມຮັບຜິດຊອບຂອງຜູ້ໃຫ້ບໍລິການ ຕ້ອງກຳນົດມາດຕະການ ດ້ານຄວາມປອດໄພດັ່ງນີ້:

1. ນຳໃຊ້ລະບົບປະຕິບັດການ (OS) ທີ່ມີຄວາມເຊື່ອຖືໄດ້ ໃນການຕິດຕັ້ງໃຫ້ຜູ້ມາໃຊ້ບໍລິການເຊົ່າເຊີເວີຈຳລອງ (Virtual Private Server (VPS)), ພ້ອມທັງອັບເດດໃຫ້ພ້ອມໃຊ້ງານ.
2. ເປີດການນຳໃຊ້ firewall ພ້ອມທັງຕັ້ງຄ່າ ໃຫ້ມີການອັບເດດອັດຕະໂນມັດ, ຕິດຕັ້ງ Anti-Virus, Anti-ransomware.
3. ກຳນົດສິດການເຂົ້າເຖິງລະບົບບໍລິຫານຈັດການ (Administrator/Root) ດ້ວຍໝາຍ IP ສະເພາະ.
4. ກຳນົດລະຫັດຜ່ານ (Password) ຕາມຄຳແນະນຳການຕັ້ງຄ່າລະຫັດຜ່ານ ຂອງ ສອຊ.
5. ເປີດ ຫຼື ປິດ Port ແລະ Services ຕາມການສະເໜີຂອງຜູ້ໃຊ້ບໍລິການ.
6. ຕິດຕາມ, ກວດກາ ແລະ ລາຍງານ ການເຮັດວຽກຂອງລະບົບການໃຫ້ບໍລິການ ຢ່າງເປັນປົກກະຕິ.
7. ຕິດຕາມ, ກວດກາ ແລະ ລາຍງານ ການເຮັດວຽກຂອງສະໜອງ Internet, ລະບົບ Firewall ແລະ ລະບົບ ພື້ນຖານໂຄ່ງລ່າງ ສອຊ ຢ່າງເປັນປົກກະຕິ.

ຂ. ຄວາມຮັບຜິດຊອບຂອງຜູ້ໃຊ້ບໍລິການ ຕ້ອງກຳນົດມາດຕະການ ດ້ານຄວາມປອດໄພດັ່ງນີ້:

1. ອັບເດດລະບົບປະຕິບັດການທີ່ຕິດຕັ້ງຢູ່ເປັນປະຈຳ ເພື່ອຮັບກັນແກ້ໄຂຈຸດອ່ອນດ້ານຄວາມປອດໄພຫຼ້າສຸດ.
2. ຮັບປະກັນໃນການຄຸ້ມຄອງລະບົບປະຕິບັດການ ແລະ ຊອຟແວໃຫ້ທັນສະໄໝທີ່ສຸດ, ໂດຍສະເພາະໃນດ້ານຄວາມປອດໄພ ແລະ ການສຳຮອງຂໍ້ມູນເປັນປະຈຳ.
3. ຕິດຕັ້ງໄຟວໍ ແລະ ກຳນົດຄ່າຢ່າງຖືກຕ້ອງເພື່ອອະນຸຍາດສະເພາະການເຊື່ອມຕໍ່ທີ່ຈຳເປັນເທົ່ານັ້ນ.
4. ຕິດຕັ້ງ ຊອຟແວຮັກສາຄວາມປອດໄພ (Anti-Virus, Anti-ransomware, Network Security) ທີ່ໄດ້ຮັບມາດຕະຖານ ແລະ ມີການອັບເດດເປັນປະຈຳ.

5. ກຳນົດສິດຂອງຜູ້ໃຊ້ ແລະ ອະນຸຍາດ ສະເພາະໝາຍເລກໄອພີ ທີ່ຕ້ອງການໃຫ້ສາມາດເຂົ້ານຳໃຊ້ລະບົບ.
6. ປິດ Port ແລະ Services ທີ່ບໍ່ຈຳເປັນ.

ມາດຕາ 08: ການສຳຮອງ ແລະ ກູ້ຄືນຂໍ້ມູນ.

ກ. ຄວາມຮັບຜິດຊອບຂອງຜູ້ໃຫ້ບໍລິການ ໃນການ ສຳຮອງ ແລະ ກູ້ຄືນຂໍ້ມູນ ດັ່ງນີ້:

1. ກວດກາລະບົບສຳຮອງຂໍ້ມູນໃຫ້ເຮັດວຽກເປັນປົກກະຕິ.
2. ກຳນົດນະໂນບາຍການສຳຮອງຂໍ້ມູນຕາມເງື່ອນໄຂທີ່ເໝາະສົມ.
3. ກວດກາພື້ນທີ່ໃນການສຳຮອງຂໍ້ມູນຂອງລະບົບເປັນປະຈຳ.
4. ຮັບປະກັນການສຳຮອງຂໍ້ມູນ, ທົດສອບການກູ້ຄືນຂໍ້ມູນໃຫ້ມີປະສິດທິຜົນ ຮັບປະກັນການກູ້ຄືນຂໍ້ມູນຂອງລະບົບ.

ຂ. ຄວາມຮັບຜິດຊອບຂອງຜູ້ໃຊ້ບໍລິການ ໃນການ ສຳຮອງ ແລະ ກູ້ຄືນຂໍ້ມູນ ດັ່ງນີ້:

1. ຮັບຜິດຊອບໃນການສຳຮອງຂໍ້ມູນຂອງຕົນເອງຢ່າງເປັນປະຈຳ ທັງຢູ່ພາຍໃນລະບົບ ແລະ ນຳອອກໄປເກັບໄວ້ນອກລະບົບ.
2. ສຳຮອງຂໍ້ມູນໄວ້ທາງໃນ ແລະ ນອກລະບົບເພື່ອຮັບປະກັນການສູນເສຍຂໍ້ມູນ.
3. ຮັບປະກັນການສຳຮອງຂໍ້ມູນທີ່ຄົບຖ້ວນ ແລະ ເກັບຮັກສາຂໍ້ມູນໄວ້ຢ່າງໜ້ອຍສອງບ່ອນທີ່ແຕກຕ່າງກັນ.
4. ຕິດຕັ້ງລະບົບ ຫຼື ສ້າງຂັ້ນຕອນການສຳຮອງຂໍ້ມູນ, ກຳນົດວິທີການສຳຮອງຂໍ້ມູນຢ່າງລະອຽດ.
5. ມີການທົດລອງ, ທົດສອບການກູ້ຄືນລະບົບ, ກູ້ຄືນຂໍ້ມູນເປັນປະຈຳ.
6. ຮັບຜິດຊອບຕໍ່ການເສຍຫາຍຂອງຂໍ້ມູນ ທີ່ເກີດຈາກຂໍ້ຜິດພາດໃນການສຳຮອງຂໍ້ມູນຂອງຕົນ.

ມາດຕາ 09: ການຍົກເລີກບໍລິການ.

1. ໃນກໍລະນີທີ່ພົບເຫັນການລະເມີດ ມາດຕະການຮັກສາຄວາມປອດໄພ ແລະ ການສຳຮອງຂໍ້ມູນ ການບໍລິການຂອງ ສູນອິນເຕີເນັດ ແຫ່ງຊາດ ແລະ ສອຊ ຂໍສະຫງວນສິດໃນການແທນຄືນຄ່າບໍລິການໃຫ້ຜູ້ຊົມໃຊ້.
2. ການນຳໃຊ້ການບໍລິການຂອງ ສອຊ ທີ່ຜິດຕໍ່ລະບຽບກົດໝາຍ, ຂັດຕໍ່ລະບຽບການຕ່າງໆຂອງ ສອຊ ສາມາດລະງັບ ຫຼື ຢຸດການໃຫ້ບໍລິການທັນທີໂດຍບໍ່ຕ້ອງແຈ້ງໃຫ້ຊາບລ່ວງໜ້າ.
3. ສອຊ ຂໍສະຫງວນສິດໃນການຍົກເລີກການໃຫ້ບໍລິການໂດຍບໍ່ຕ້ອງແຈ້ງໃຫ້ຊາບລ່ວງໜ້າ ໃນກໍລະນີທີ່ມີການລະເມີດກົດລະບຽບສະບັບນີ້.

ມາດຕາ 10: ຜົນສັກສິດ

ກົດລະບຽບສະບັບນີ້ ມີຜົນສັກສິດ ແລະ ນຳໃຊ້ນັບແຕ່ມື້ລົງລາຍເຊັນເປັນຕົ້ນໄປ.

ທ້າວໜ້າສຸນ

ມິນາໄຊ ພິລາວົງ