ສາທາລະນະລັດ ປະຊາທິປະໄຕ ປະຊາຊົນລາວ
ສັນຕິພາບ ເອກະລາດ ປະຊາທິປະໄຕ ເອກະພາບ ວັດທະນະຖາວອນ

ກະຊວງ ໄປສະນີ, ໂທລະຄົມມະນາຄົມ ແລະ ການສື່ສານ

ເລກທີ 3623 /ປທສ
ນະຄອນຫຼວງວຽງຈັນ, ວັນທີ 11 ທັນວາ 2017

ຄຳແນະນຳ
ກ່ຽວກັບ ການຮັກສາຄວາມປອດໄພທາງລະບົບຄອມພິວເຕີ

- ອີງຕາມ ກົດໝາຍ ສະບັບເລກທີ 61/ສພຊ, ລົງວັນທີ 15 ກໍລະກົດ 2015, ວ່າດ້ວຍ ການຕ້ານ ແລະ ສະກັດກັ້ນອາຊະຍາກຳທາງລະບົບຄອມພິວເຕີ.
- ອີງຕາມ ດຳລັດ ຂອງ ນາຍົກລັດຖະມົນຕີ ສະບັບເລກທີ 22/ນຍ, ລົງວັນທີ 16 ມັງກອນ 2017 ວ່າດ້ວຍ: ການຈັດຕັ້ງ ແລະ ເຄື່ອນໄຫວຂອງ ກະຊວງ ໄປສະນີ, ໂທລະຄົມມະນາຄົມ ແລະ ການສື່ສານ.

ລັດຖະມົນຕີ ອອກຄຳແນະນຳ:

I. ຈຸດປະສົງ

ຄຳແນະນຳສະບັບນີ້ ວາງອອກເພື່ອຜັນຂະຫຍາຍເນື້ອໃນ ມາດຕາ 27 ຂອງກົດໝາຍ ວ່າດ້ວຍການຕ້ານ ແລະ ສະກັດກັ້ນອາຊະຍາກຳທາງລະບົບຄອມພິວເຕີ ກ່ຽວກັບມາດຕະການສະເພາະໃນການຮັກສາຄວາມປອດໄພທາງລະບົບຄອມພິວເຕີ ເພື່ອໃຫ້ການສ້າງ, ປ້ອງກັນ, ຄຸ້ມຄອງ, ຕິດຕາມ ແລະ ກວດກາຄວາມປອດໄພຂອງລະບົບຄອມພິວເຕີ ເປັນເອກະພາບໃນຂອບເຂດທົ່ວປະເທດ.

II. ການສ້າງ ແລະ ການປ້ອງກັນເຄືອຂ່າຍຄອມພິວເຕີ

1. ການສ້າງເຄືອຂ່າຍຄອມພິວເຕີ

ການສ້າງເຄືອຂ່າຍຄອມພິວເຕີໃຫ້ມີຄວາມປອດໄພ ເພື່ອນຳໃຊ້ເຂົ້າໃນວຽກງານການຄຸ້ມຄອງ, ການບໍລິຫານ, ການບໍລິການ, ການນຳໃຊ້ຂໍ້ມູນຂ່າວສານ ແລະ ອິນເຕີເນັດ ຜູ້ຄຸ້ມຄອງເຄືອຂ່າຍຄອມພິວເຕີ ຄວນປະຕິບັດດັ່ງນີ້:

1.1. ສ້າງແຜນຜັງ ເຄືອຂ່າຍຄອມພິວເຕີ (Network Diagram) ເພື່ອສະດວກໃນການຄຸ້ມຄອງ, ການຕິດຕັ້ງ, ສ້ອມແປງ ແລະ ການບຳລຸງຮັກສາ;

1.2. ສ້າງເຄືອຂ່າຍຄອມພິວເຕີໃຫ້ເປັນແຕ່ລະພາກສ່ວນສະເພາະ ຕາມການໃຊ້ງານເຊັ່ນ: ເຄືອຂ່າຍຄອມພິວເຕີພາຍໃນ ແລະ ພາຍນອກ ເພື່ອໃຫ້ສາມາດຕິດຕາມກວດກາໄພຄຸກຄາມ ການບຸກລຸກໄດ້ຢ່າງເປັນລະບົບ;

1.3. ກວດກາ ບັນດາອຸປະກອນທີ່ຈະນຳມາຕິດຕັ້ງຢູ່ໃນເຄືອຂ່າຍຄອມພິວເຕີ ແລະ ລະບົບຄອມພິວເຕີແມ່ຂ່າຍ ເປັນຕົ້ນ ກວດກາໄວຣັດຄອມພິວເຕີ ແລະ ການກຳນົດຄ່າຕ່າງໆທາງເຕັກນິກຂອງບັນດາອຸປະກອນເຫຼົ່ານັ້ນ;

1.4. ຕິດຕັ້ງໂປຣແກຣມສຳລັບຕິດຕາມສະຖານະພາບການເຮັດວຽກຂອງແຕ່ລະອຸປະກອນທີ່ເຊື່ອມຕໍ່ເຂົ້າກັບລະບົບເຄືອຂ່າຍ;

1.5. ການເຂົ້າເຖິງເຄືອຂ່າຍຄອມພິວເຕີພາຍໃນອົງກອນ ໂດຍຜ່ານທາງລະບົບອິນເຕີເນັດ ຕ້ອງໄດ້ບັນທຶກການເຂົ້າເຖິງລະບົບທຸກຄັ້ງ (Login) ແລະ ຕ້ອງຢັ້ງຢືນຕົວຕົນ (Authentication) ໃຫ້ຖືກຕ້ອງ;

1.6. ຫ້າມເຄື່ອນຍ້າຍ ຫຼື ຕິດຕັ້ງອຸປະກອນເພີ່ມ ເຊັ່ນ: ອຸປະກອນເຊື່ອມຕໍ່ເຄືອຂ່າຍ, ອຸປະກອນເຊື່ອມໂຍງຄອມພິວເຕີ, ລະບົບຄອມພິວເຕີແມ່ຂ່າຍ ຫຼື ອຸປະກອນ ອື່ນໆ ໂດຍບໍ່ໄດ້ຮັບອະນຸຍາດຈາກຜູ້ຄຸ້ມຄອງລະບົບ.

2. ການປ້ອງກັນລະບົບຄອມພິວເຕີແມ່ຂ່າຍ

ເພື່ອຮັບປະກັນລະບົບຄອມພິວເຕີແມ່ຂ່າຍ ໃຫ້ສາມາດສະໜອງຂໍ້ມູນຂ່າວສານສະດວກວ່ອງໄວ ແລະ ຖືກຕ້ອງ ຜູ້ຄຸ້ມຄອງລະບົບຄອມພິວເຕີແມ່ຂ່າຍຄວນປະຕິບັດ ດັ່ງນີ້:

2.1. ກຳນົດນະໂຍບາຍການຮັກສາຄວາມປອດໄພທີ່ສາມາດຄວບຄຸມ, ເຂົ້າເຖິງ ຫຼື ປ້ອງກັນການຈະລາຈອນຂໍ້ມູນ ທີ່ອາດສິ່ງຜົນກະທົບຕໍ່ລະບົບຄອມພິວເຕີແມ່ຂ່າຍ;

2.2. ບັນທຶກຄ່າປ່ຽນແປງຕ່າງໆ ຂອງເຄື່ອງແມ່ຂ່າຍຕະຫຼອດ 24/7 ຊົ່ວໂມງ ຫຼື ທຸກຄັ້ງທີ່ມີການປ່ຽນແປງການຕັ້ງຄ່າໃຫ້ລະບົບຄອມພິວເຕີແມ່ຂ່າຍ;

2.3. ມີຂັ້ນຕອນ ຫຼື ວິທີປະຕິບັດ ໃນການກວດກາຄວາມປອດໄພລະບົບລະບົບຄອມພິວເຕີແມ່ຂ່າຍ ຖ້າຫາກກວດພົບສິ່ງຜິດປົກກະຕິ ຫຼື ມີການປ່ຽນແປງຄ່າຕ່າງໆ ຈະຕ້ອງໄດ້ດຳເນີນການແກ້ໄຂໂດຍດ່ວນ;

2.4. ບັນທຶກການປະຕິບັດການຂອງລະບົບຄອມພິວເຕີແມ່ຂ່າຍ ທີ່ຜິດປົກກະຕິ, ບັນທຶກການເຮັດວຽກຂອງຜູ້ໃຊ້ງານ ແລະ ບັນທຶກການ ເຂົ້າ-ອອກ ລະບົບ;

2.5. ແຕ່ງຕັ້ງບຸກຄົນຮັບຜິດຊອບລະບົບຄອມພິວເຕີແມ່ຂ່າຍສະເພາະ ເພື່ອຕັ້ງຄ່າ, ແກ້ໄຂ ຫຼື ປ່ຽນແປງຄ່າໃຫ້ລະບົບຄອມພິວເຕີແມ່ຂ່າຍປະຕິບັດການ ດ້ວຍຄວາມຮັບຜິດຊອບ;

2.6. ກຳນົດເສັ້ນທາງບໍລິການທີ່ຈຳເປັນ ໃຫ້ແກ່ການເຂົ້າເຖິງ, ນຳໃຊ້, ປັບປຸງ, ຕັ້ງຄ່າ, ແກ້ໄຂ ຫຼື ປ່ຽນແປງຄ່າໃນລະບົບຄອມພິວເຕີແມ່ຂ່າຍ ເພື່ອຫຼຸດຜ່ອນຄວາມສ່ຽງການບຸກລຸກທຳລາຍລະບົບຄອມພິວເຕີແມ່ຂ່າຍ;

2.7. ການເຂົ້າເຖິງລະບົບລະບົບຄອມພິວເຕີແມ່ຂ່າຍ ຈາກພາຍນອກ (Remote login) ຫຼື ການເຂົ້າຫາອຸປະກອນເຄືອຂ່າຍພາຍໃນ ດ້ວຍຮູບແບບ FTP, FTPS, SSH ຕ້ອງໃຫ້ສອດຄອງກັບນະໂຍບາຍຂອງອົງກອນ.

3. ການປ້ອງກັນເຄືອຂ່າຍຄອມພິວເຕີໃຊ້ສາຍ

ເພື່ອຮັບປະກັນໃຫ້ເຄືອຂ່າຍຄອມພິວເຕີທີ່ເຊື່ອມຕໍ່ກັບລະບົບຄອມພິວເຕີແມ່ຂ່າຍ ໃຫ້ມີຄວາມປອດໄພ ຜູ້ຄຸ້ມຄອງເຄືອຂ່າຍຄອມພິວເຕີ ແລະ ຜູ້ຄຸ້ມຄອງລະບົບຄອມພິວເຕີແມ່ຂ່າຍ ຄວນປະຕິບັດດັ່ງນີ້:

3.1. ຕິດຕັ້ງ ແລະ ນຳໃຊ້ອຸປະກອນທີ່ໄດ້ມາດຕະຖານສາກົນ;

3.2. ຕິດຕັ້ງລະບົບກວດຈັບການບຸກລຸກ (Intrusion Prevention System/Intrusion Detection System) ເພື່ອກວດສອບການບຸກລຸກເຄືອຂ່າຍຄອມພິວເຕີ ແລະ ຊອກຫາວິທີການໃນການປ້ອງກັນລະບົບຄອມພິວເຕີໃຫ້ມີຄວາມປອດໄພ;

3.3. ຕິດຕັ້ງລະບົບປ້ອງກັນການໂຈມຕີແບບ DDoS ໃຫ້ປະກອບມີລະບົບຄົ້ນຫາການບຸກລຸກ ແລະ ລະບົບກຳຈັດການບຸກລຸກ ເພື່ອປ້ອງກັນບໍ່ໃຫ້ລະບົບຄອມພິວເຕີແມ່ຂ່າຍ ແລະ ເຄືອຂ່າຍຄອມພິວເຕີ ຢຸດຕິການທຳງານ;

3.4. ຕິດຕັ້ງລະບົບປ້ອງກັນ Firewall ເພື່ອກັ້ນຕອງການບຸກລຸກລະຫວ່າງເຄືອຂ່າຍພາຍໃນ ແລະ ເຄືອຂ່າຍຄອມພິວເຕີພາຍນອກ ແລະ ຕັ້ງຄ່າການຈັດເກັບຂໍ້ມູນຈະລາຈອນ ເຂົ້າ-ອອກ ເຄືອຂ່າຍຄອມພິວເຕີ ໄວ້ໃນລະບົບຈັດເກັບຂໍ້ມູນ (Log Management System) ເພື່ອກວດສອບ, ວິເຄາະຂໍ້ມູນການບຸກລຸກ ແລະ ວາງແຜນການປ້ອງກັນ;

3.5. ການເຂົ້າເຖິງເຄືອຂ່າຍຄອມພິວເຕີຈາກພາຍນອກ ຕ້ອງໄດ້ຮັບອະນຸຍາດຈາກຜູ້ຄຸ້ມຄອງລະບົບ ແລະ ມີການຄວບຄຸມຢ່າງເຂັ້ມງວດເຊັ່ນ: ການກວດສອບຕົວຕົນ ແລະ ສິດຂອງຜູ້ໃຊ້ງານ;

3.6. ການກວດສອບການປະຕິບັດການຂອງເຄືອຂ່າຍຄອມພິວເຕີໃນແຕ່ລະຄັ້ງ ຕ້ອງໄດ້ຮັບອະນຸຍາດຈາກຜູ້ຄຸ້ມຄອງລະບົບ ຫຼື ຫົວໜ້າອົງກອນ;

3.7. ການແກ້ໄຂ ຫຼື ປ່ຽນແປງຄ່າຂອງອຸປະກອນໃນເຄືອຂ່າຍຄອມພິວເຕີ ຜູ້ຄຸ້ມຄອງເຄືອຂ່າຍຄອມພິວເຕີ ຕ້ອງແຈ້ງໃຫ້ວິຊາການເຕັກນິກພາຍໃນຂອງຕົນ ເພື່ອຮັບຮູ້ ແລະ ປະຕິບັດຕາມ;

3.8. ມີແຜນເວລາໃນການຕິດຕາມ, ກວດກາ, ບຳລຸງຮັກສາ ແລະ ປັບປຸງ ເຄືອຂ່າຍຄອມພິວເຕີ ຕ້ອງປະຕິບັດ ແຕ່ 3 ຫາ 6 ເດືອນ ຕໍ່ ຄັ້ງ ຕໍ່ ປີ.

4. ການປ້ອງກັນເຄືອຂ່າຍຄອມພິວເຕີບໍ່ໃຊ້ສາຍ

ເພື່ອຮັບປະກັນໃຫ້ເຄືອຂ່າຍຄອມພິວເຕີ ທີ່ເຊື່ອມຕໍ່ກັບລະບົບຄອມພິວເຕີແມ່ຂ່າຍ ໂດຍນຳໃຊ້ເຄືອຂ່າຍຄອມພິວເຕີບໍ່ໃຊ້ສາຍ ເພື່ອເຂົ້າບໍລິຫານຈັດການກັບລະບົບຄອມພິວເຕີແມ່ຂ່າຍໃຫ້ມີຄວາມປອດໄພ ຄວນປະຕິບັດດັ່ງນີ້:

4.1. ຕິດຕັ້ງ ແລະ ນຳໃຊ້ອຸປະກອນທີ່ໄດ້ມາດຕະຖານສາກົນ;

4.2. ກຳນົດລະຫັດການເຂົ້າໃຊ້ງານ ເພື່ອຄວບຄຸມສັນຍານຂອງອຸປະກອນກະຈາຍສັນຍານ ບໍ່ໃຊ້ສາຍ (Wi-Fi) ແລະ ເຂົ້າລະຫັດການເຂົ້ານຳໃຊ້ (Authentication);

4.3. ຕິດຕັ້ງອຸປະກອນກະຈາຍສັນຍານບໍ່ໃຊ້ສາຍໃນຕຳແໜ່ງທີ່ເໝາະສົມ, ຕັ້ງຄ່າກຳນົດຂອບເຂດພື້ນທີ່ການໃຊ້ງານ ເພື່ອໃຫ້ມີຄວາມສະດວກວ່ອງໄວ ແລະ ງ່າຍໃນການບຳລຸງຮັກສາ;

4.4. ບໍ່ອະນຸຍາດໃຫ້ຜູ້ໃຊ້ງານ ນຳອຸປະກອນເຄືອຂ່າຍບໍ່ໃຊ້ສາຍມາຕິດຕັ້ງ ຫຼື ເປີດໃຊ້ງານເອງໃນອົງກອນ ເປັນຕົ້ນ: Access point, Wireless Router, Wireless card;

4.5. ກຳນົດລະຫັດເຄື່ອງຄອມພິວເຕີ (MAC Address) ທີ່ສາມາດເຂົ້າໃຊ້ລະບົບກະຈາຍສັນຍານບໍ່ໃຊ້ສາຍໄດ້ສະເພາະເຄື່ອງຄອມພິວເຕີທີ່ອະນຸຍາດ ຫຼື ຕາມລາຍຊື່ທີ່ອະນຸຍາດ ໂດຍມີລະຫັດຜ່ານຕາມທີ່ກຳນົດໄວ້ຢູ່ພາຍໃນອົງກອນ;

4.6. ປ່ຽນຊື່ສັນຍານບໍ່ໃຊ້ສາຍທີ່ໃຫ້ບໍລິການ Service Set Identifier (SSID) ທີ່ກຳນົດຊື່ມາຈາກໂຮງງານຜະລິດມາເປັນຊື່ຂອງອົງກອນ;

4.7. ຕັ້ງຄ່າອຸປະກອນກະຈາຍສັນຍານບໍ່ໃຊ້ສາຍໃຫ້ເໝາະສົມ ຕາມລາຍການໃນການຕັ້ງຄ່າມາດຕະຖານຄວາມປອດໄພຂອງອຸປະກອນ;

4.8. ຕັ້ງຄ່າອຸປະກອນກະຈາຍສັນຍານບໍ່ໃຊ້ສາຍໃນສ່ວນການປ້ອງກັນການເຂົ້ານຳໃຊ້ສັນຍານ WPA2 (Wireless Protected Access 2) ດ້ວຍການເຂົ້າລະຫັດປ້ອງກັນ;

4.9. ກຳນົດລະບຽບການ ເຂົ້າໃຊ້ງານລະບົບເຄືອຂ່າຍບໍ່ໃຊ້ສາຍຂອງອົງກອນ;

4.10. ມີຊອບແວ ຫຼື ຮາດແວ ເພື່ອນຳໃຊ້ເຂົ້າໃນການກວດສອບຄວາມປອດໄພຂອງລະບົບເຄືອຂ່າຍບໍ່ໃຊ້ສາຍ ແລະ ບັນທຶກການນຳໃຊ້ທີ່ຜິດປົກກະຕິ;

4.11. ໃນກໍລະນີ ທີ່ກວດເຫັນການໃຊ້ງານລະບົບເຄືອຂ່າຍບໍ່ໃຊ້ສາຍທີ່ຜິດປົກກະຕິ ໃຫ້ແຈ້ງຕໍ່ຜູ້ຄຸ້ມຄອງເຄືອຂ່າຍຄອມພິວເຕີ ດຳເນີນການແກ້ໄຂທັນທີ.

5. ການປ້ອງກັນເມັລແວ

ໃນການປ້ອງກັນ ເມັລແວ ຫຼື ໄວຣັດຄອມພິວເຕີ ບໍ່ໃຫ້ແຜ່ກະຈາຍໄປທົ່ວເຄືອຂ່າຍຄອມພິວເຕີທີ່ມີການເຊື່ອມໂຍງກັນ ຜູ້ຄຸ້ມຄອງເຄືອຂ່າຍຄອມພິວເຕີ ແລະ ຜູ້ນຳໃຊ້ຄອມພິວເຕີ ຄວນປະຕິບັດ ດັ່ງນີ້:

5.1. ຕິດຕັ້ງໂປຣແກຣມປ້ອງກັນໄວຣັດຄອມພິວເຕີ ທີ່ມີການອະນຸຍາດນຳໃຊ້ (Software License) ແລະ ປັບປຸງໃຫ້ຢູ່ໃນສະພາບການໃຊ້ງານ;

5.2. ເປີດນຳໃຊ້ ວິນໂດໄຟວໍ (Windows Firewall) ທີ່ມາພ້ອມກັບລະບົບປະຕິບັດການວິນໂດ ເພື່ອປ້ອງກັນການບຸກລຸກຂອງໄວຣັດ;

5.3. ເປີດນຳໃຊ້ໂປຣແກຣມກວດຈັບ ຫຼື ໂປຣແກຣມປ້ອງກັນໄວຣັດ ທີ່ມາພ້ອມກັບລະບົບປະຕິບັດການ ເປັນຕົ້ນ Windows Defender;

5.4. ກວດກາ ແລະ ກຳຈັດ ໄວຣັດຄອມພິວເຕີຢູ່ຝ່າຍຂໍ້ມູນ ແລະ ເອກະສານອື່ນໆ ກ່ອນການນຳໃຊ້ ຫຼື ບັນທຶກຝ່າຍຂໍ້ມູນລົງໃນອຸປະກອນບັນທຶກຂໍ້ມູນ;

5.5. ກວດກາ ແລະ ກຳຈັດ ໄວຣັດຄອມພິວເຕີຢູ່ອຸປະກອນໜ່ວຍຄວາມຈຳພາຍນອກ ເຊັ່ນ: External harddisk, Memory stick ແລະ ອື່ນໆ ກ່ອນນຳໄປໃຊ້ງານ;

5.6. ບໍ່ກົດລິ້ງ ແລະ ເປີດຝ່າຍເອກະສານ ທີ່ບໍ່ຮູ້ແຫຼ່ງທີ່ມາ ຫຼື ຝ່າຍເອກະສານຄັດຕິດມາໃນຈົດໝາຍເອເລັກໂຕຣນິກ ໂດຍບໍ່ມີທີ່ຢູ່ຂອງຜູ້ສົ່ງ;

5.7. ບໍ່ເຂົ້າເຖິງເວັບໄຊ ແລະ ດາວໂຫຼດໂປຣແກຣມຄອມພິວເຕີຈາກເວັບໄຊທີ່ບໍ່ຮູ້ແຫຼ່ງທີ່ມາ ແລະ ບໍ່ໜ້າເຊື່ອຖື;

5.8. ໃນກໍລະນີທີ່ພົບເຫັນໄວຣັດ ໃຫ້ດຳເນີນການແກ້ໄຂ ແລະ ກຳຈັດໄວຣັດຄອມພິວເຕີທັນທີ ຫຼື ແຈ້ງຫາພາກສ່ວນທີ່ກ່ຽວຂ້ອງດຳເນີນການແກ້ໄຂໂດຍດ່ວນ.

III. ການຄຸ້ມຄອງການນຳໃຊ້ເຄືອຂ່າຍຄອມພິວເຕີ

1. ການກຳນົດລາຍຊື່ຜູ້ໃຊ້ຄອມພິວເຕີ

ຜູ້ຄຸ້ມຄອງເຄືອຂ່າຍຄອມພິວເຕີ ຄວນກຳນົດ ສິດ, ຂອບເຂດ ແລະ ບັນທຶກລາຍຊື່ຜູ້ໃຊ້ງານ ໃຫ້ສາມາດ ກວດກາ, ຕິດຕາມການເຂົ້ານຳໃຊ້ເຄືອຂ່າຍຄອມພິວເຕີ ດັ່ງນີ້:

1.1. ການເຂົ້າເຖິງເຄືອຂ່າຍຄອມພິວເຕີ;

1.2. ການເຂົ້າເຖິງຝ່າຍຂໍ້ມູນສຳຄັນຕ່າງໆ ໃນລະບົບຄຸ້ມຄອງເອກະສານ;

1.3. ການນຳໃຊ້ໂປຣແກຣມສະເພາະ ເປັນຕົ້ນ ໂປຣແກຣມບັນຊີ, ຄຸ້ມຄອງພະນັກງານ, ຖານຂໍ້ມູນຄອມພິວເຕີ ແລະ ອື່ນໆ;

1.4. ໃຫ້ຢຸດເຊົາ ຫຼື ລຶບ ບັນຊີ ຜູ້ໃຊ້ເຄືອຂ່າຍຄອມພິວເຕີ ທີ່ບໍ່ມີພັນທະກ່ຽວຂ້ອງກັບອົງກອນ ດັ່ງກ່າວໂດຍທັນທີ;

1.5. ຜູ້ທີ່ບໍ່ມີພັນທະກ່ຽວຂ້ອງກັບອົງກອນແລ້ວ ບໍ່ອະນຸຍາດໃຫ້ສຳເນົາ, ທຳລາຍ ຫຼື ປ່ຽນແປງ ຂໍ້ມູນພາຍໃນອົງກອນ.

2. ການກຳນົດລະຫັດການເຂົ້າໃຊ້ງານຄອມພິວເຕີ

ການເຂົ້າເຖິງເຄືອຂ່າຍຄອມພິວເຕີ ຜູ້ຄຸ້ມຄອງເຄືອຂ່າຍຄອມພິວເຕີ ຫຼື ເຈົ້າຂອງຄອມພິວເຕີ ຄວນກຳນົດລະຫັດຜ່ານເຂົ້າໃຊ້ງານເຄືອຂ່າຍຄອມພິວເຕີ ດັ່ງນີ້:

2.1. ການຕັ້ງລະຫັດຜ່ານໃຫ້ລວມມີທັງຕົວເລກ, ຕົວອັກສອນ (ໃຫຍ່-ນ້ອຍ) ແລະ ສັນຍະລັກ ຫຼື ເຄື່ອງໝາຍ ເປັນຕົ້ນ #% $ @;

2.2. ກຳນົດໃຫ້ລະຫັດຜ່ານມີຄວາມຍາວຢ່າງໜ້ອຍ 8 ຕົວອັກສອນຂຶ້ນໄປ;

2.3. ບໍ່ຄວນກຳນົດລະຫັດຜ່ານທີ່ມີລັກສະນະຄາດເດົາໄດ້ງ່າຍເຊັ່ນ: abcdef, aaaaaa, 123456;

2.4. ບໍ່ຄວນກຳນົດລະຫັດຜ່ານທີ່ກ່ຽວຂ້ອງກັບຂໍ້ມູນສ່ວນຕົວຂອງຜູ້ໃຊ້ງານເຊັ່ນ: ຊື່, ນາມສະກຸນ, ວັນເດືອນ ປີເກີດ ແລະ ໝາຍເລກໂທລະສັບ;

2.5. ບໍ່ອະນຸຍາດໃຫ້ຜູ້ອື່ນນຳໃຊ້ຊື່ຜູ້ໃຊ້ ແລະ ລະຫັດຜ່ານຂອງຕົນ;

2.6. ບໍ່ຄວນກຳນົດລະຫັດຜ່ານທີ່ຢູ່ໃນວັດຈະນານຸກົມ;

2.7. ສຳລັບຜູ້ຄຸ້ມຄອງລະບົບ ໃຫ້ປ່ຽນລະຫັດຜ່ານ 3 ເດືອນຕໍ່ຄັ້ງ;

2.8. ສຳລັບຜູ້ໃຊ້ງານທົ່ວໄປ ໃຫ້ປ່ຽນລະຫັດຜ່ານ 6 ເດືອນຕໍ່ຄັ້ງ.

3. ການນຳໃຊ້ຈົດໝາຍເອເລັກໂຕຣນິກ

ການນຳໃຊ້ຈົດໝາຍເອເລັກໂຕຣນິກ ໃຫ້ຖືກວິທີ ແລະ ປອດໄພຄວນປະຕິບັດ ດັ່ງນີ້:

3.1. ນຳໃຊ້ຈົດໝາຍເອເລັກໂຕຣນິກທີ່ສ້າງຂຶ້ນ ແລະ ຄຸ້ມຄອງໂດຍອົງກອນຂອງຕົນ;

3.2. ປ່ຽນລະຫັດຜ່ານທັນທີ ເມື່ອນຳໃຊ້ລະບົບຈົດໝາຍເອເລັກໂຕຼນິກໃນຄັ້ງທຳອິດ;

3.3. ປ່ຽນລະຫັດການເຂົ້າໃຊ້ຈົດໝາຍເອເລັກໂຕຣນິກ ຄວນປະຕິບັດຕາມຕາມຂໍ້ທີ 2 ຂອງພາກທີ III ຂ້າງເທິງ;

3.4. ເຂົ້າລະຫັດໃຫ້ກັບຂໍ້ມູນທີ່ເປັນຄວາມລັບ ກ່ອນສົ່ງຜ່ານທາງຈົດໝາຍເອເລັກໂຕຣນິກ;

3.5. ບໍ່ບັນທຶກ ຫຼື ຮັກສາລະຫັດຜ່ານໄວ້ໃນລະບົບຄອມພິວເຕີ ຫຼື ເກັບໄວ້ໃນບ່ອນທີ່ສັງເກດໄດ້ງ່າຍ;

3.6. ບໍ່ນຳໃຊ້ທີ່ຢູ່ຈົດໝາຍເອເລັກໂຕຣນິກຂອງບຸກຄົນອື່ນ ໂດຍບໍ່ໄດ້ຮັບອະນຸຍາດ;

3.7. ບໍ່ປອມແປງຊື່ບັນຊີຂອງຜູ້ສົ່ງ ໂດຍການປົກປິດທີ່ຢູ່ ຫຼື ແຫຼ່ງທີ່ມາຂອງຈົດໝາຍເອເລັກໂຕຣນິກຂອງຕົນ;

3.8. ບໍ່ນຳໃຊ້ຈົດໝາຍເອເລັກໂຕຣນິກຂອງອົງກອນ ເພື່ອໄປສະໝັກໃນເວັບໄຊທີ່ໃຫ້ບໍລິການທາງອິນເຕີເນັດ;

3.9. ຫຼັງຈາກນຳໃຊ້ລະບົບຈົດໝາຍເອເລັກໂຕຣນິກແລ້ວ ຄວນອອກຈາກລະບົບ (Logout) ທຸກຄັ້ງ.

4. ການນຳໃຊ້ອິນເຕີເນັດ

ການນຳໃຊ້ອິນເຕີເນັດໃຫ້ມີຄວາມປອດໄພ ຜູ້ຄຸ້ມຄອງເຄືອຂ່າຍຄອມພິວເຕີ ແລະ ຜູ້ໃຊ້ງານອິນເຕີເນັດ ຄວນປະຕິບັດ ດັ່ງນີ້:

4.1. ກຳນົດ, ອອກລະບຽບການນຳໃຊ້ອິນເຕີເນັດພາຍໃນອົງກອນ ເພື່ອຄວາມສະດວກໃນການຄຸ້ມຄອງ, ກວດກາ ແລະ ຕິດຕາມ;

4.2. ຜູ້ຄຸ້ມຄອງເຄືອຂ່າຍຄອມພິວເຕີ ຕ້ອງກຳນົດເສັ້ນທາງການເຊື່ອມຕໍ່ອິນເຕີເນັດ ໃຫ້ຜູ້ໃຊ້ງານພາຍໃນອົງກອນໃຫ້ຜ່ານລະບົບປ້ອງກັນຄວາມປອດໄພ (Firewall system);

4.3. ຜູ້ຄຸ້ມຄອງເຄືອຂ່າຍຄອມພິວເຕີ ຕ້ອງກຳນົດສິດໃນການເຂົ້າເຖິງແຫຼ່ງຂໍ້ມູນ ຕາມໜ້າທີ່ຄວາມຮັບຜິດຊອບຕາມລະບຽບການຂອງອົງກອນທີ່ໄດ້ກຳນົດໄວ້;

4.4. ຜູ້ໃຊ້ງານອິນເຕີເນັດ ຕ້ອງກວດສອບຄວາມຖືກຕ້ອງຂອງຂໍ້ມູນທີ່ນຳມາຈາກ ອິນເຕີເນັດກ່ອນນຳໄປໃຊ້ງານ;

4.5. ໃນກໍລະນີ ຜູ້ໃຊ້ອິນເຕີເນັດເຂົ້າເຖິງລະບົບຖານຂໍ້ມູນ ຜ່ານໂປຣແກຣມເຂົ້າໃຊ້ງານອິນເຕີເນັດ (Web Browser) ພາຍຫຼັງສຳເລັດພາລະກິດຂອງຕົນ ຕ້ອງປິດໂປຣແກຣມເຂົ້າໃຊ້ງານອິນເຕີເນັດທັນທີ ເພື່ອປ້ອງກັນ ບໍ່ໃຫ້ບຸກຄົນອື່ນເຂົ້າເຖິງຖານຂໍ້ມູນໄດ້;

4.6. ເຂົ້າລະຫັດຂໍ້ມູນທຸກຄັ້ງ ກ່ອນສົ່ງຂໍ້ມູນຜ່ານທາງເຄືອຂ່າຍອິນເຕີເນັດ.

5. ການປຸກຈິດສຳນຶກໃນການຮັກສາຄວາມປອດໄພ

ອົງກອນ ຫຼື ໜ່ວຍງານຄຸ້ມຄອງຄວາມປອດໄພ ຄວນສ້າງກິດຈະກຳປຸກຈິດສຳນຶກໃຫ້ຜູ້ຊົມໃຊ້ເຄືອຂ່າຍຄອມພິວເຕີພາຍໃນອົງກອນ ຮັບຮູ້ເຖິງໄພຄຸກຄາມຜ່ານທາງອິນເຕີເນັດ ດັ່ງນີ້:

5.1. ອົງກອນ ຫຼື ໜ່ວຍງານຮັກສາຄວາມປອດໄພຂອງອົງກອນ ຕ້ອງຈັດຝຶກອົບຮົມການບຳລຸງຮັກສາເຄືອຂ່າຍຄອມພິວເຕີໃຫ້ແກ່ຜູ້ໃຊ້ ແລະ ຜູ້ຄຸ້ມຄອງເຄືອຂ່າຍຄອມພິວເຕີພາຍໃນອົງກອນ ຢ່າງເປັນປົກກະຕິ ເພື່ອຝຶກ

ຊ້ອມຮັບມືກັບໄພຄຸກຄາມທີ່ອາດເກີດຂຶ້ນ ແລະ ສາມາດກູ້ລະບົບຄອມພິວເຕີທີ່ຖືກເສຍຫາຍໃຫ້ກັບຄືນສູ່ສະພາບການໃຊ້ງານ;

5.2. ສ້າງຄຳຂວັນເຕືອນສະຕິໄພຄຸກຄາມທາງຄອມພິວເຕີ ເປັນຕົ້ນແມ່ນ ການສ້າງແຜ່ນໂຄສະນາ, ວາລະສານ, ວີດີໂອ, ເຄັດລັບການຮັກສາຄວາມປອດໄພ ແລະ ເຜີຍແຜ່ໃຫ້ທຸກຄົນພາຍໃນອົງກອນຮັບຊາບ;

5.3. ບໍ່ກົດ ຫຼື ສະແດງພຶດຕິກຳຮຸນແຮງກັບຄອມພິວເຕີ ເມື່ອຄອມພິວເຕີຄ້າງ ຫຼື ໂປຣແກຣມ ບໍ່ເຮັດວຽກ;

5.4. ບໍ່ສ້ອມແປງ ຫຼື ແກ້ໄຂບັນຫາທີ່ເກີດຂຶ້ນໃນລະບົບຄອມພິວເຕີຂອງອົງກອນ ໂດຍບໍ່ໄດ້ຮັບອະນຸຍາດຈາກການຈັດຕັ້ງຂອງອົງກອນ;

5.5. ຖ້າບໍ່ຮູ້ວິທີແກ້ໄຂບັນຫາທີ່ເກີດຂຶ້ນໃນລະບົບຄອມພິວເຕີຂອງຕົນ ຫຼື ອົງກອນ ຄວນແຈ້ງໃຫ້ ໜ່ວຍງານຄຸ້ມຄອງລະບົບຄອມພິວເຕີຂອງອົງກອນ ເພື່ອດຳເນີນການແກ້ໄຂ;

5.6. ອ່ານຂໍ້ຄວາມທີ່ລະບົບປະຕິບັດການແຈ້ງເຕືອນ (Pop-Up) ຂຶ້ນມາ ກ່ອນທີ່ຈະກົດຍອມຮັບ;

5.7. ອອກຈາກລະບົບບໍລິການ (Log out) ທັນທີ ເມື່ອບໍ່ໃຊ້ງານ;

5.8. ລ໋ອກໜ້າຈໍຄອມພິວເຕີເມື່ອບໍ່ມີການນຳໃຊ້ງານ;

5.9. ສຶກສາ ແລະ ປະຕິບັດຕາມຄູ່ມືແນະນຳການນຳໃຊ້ອຸປະກອນເຄືອຂ່າຍຄອມພິວເຕີ ໃຫ້ມີຄວາມປອດໄພ.

6. ການສຳຮອງຂໍ້ມູນຄອມພິວເຕີ

ເພື່ອຮັບປະກັນໃຫ້ຂໍ້ມູນຄອມພິວເຕີ ມີຄວາມປອດໄພ, ບໍ່ເສຍຫາຍ ແລະ ສາມາດນຳມາໃຊ້ງານໄດ້ເປັນປົກກະຕິ ຜູ້ຄຸ້ມຄອງເຄືອຂ່າຍຄອມພິວເຕີ ແລະ ຜູ້ນຳໃຊ້ຄອມພິວເຕີ ຄວນປະຕິບັດ ດັ່ງນີ້:

6.1. ກຳນົດຂັ້ນຕອນ ຫຼື ວິທີປະຕິບັດໃນການສຳຮອງຂໍ້ມູນ ເປັນຕົ້ນ: ຂໍ້ມູນທີ່ຕ້ອງສຳຮອງ, ປະເພດຂອງຂໍ້ມູນ, ບໍລິມາດຂໍ້ມູນທີ່ຕ້ອງການສຳຮອງ, ຂັ້ນຕອນການສຳຮອງ, ການເກັບຮັກສາຂໍ້ມູນ, ການກຳນົດເວລາເກັບຮັກສາຂໍ້ມູນ, ສະຖານທີ່ເກັບຮັກສາຂໍ້ມູນ ແລະ ບັນທຶກການປະຕິບັດງານ;

6.2. ສ້າງລະບົບສຳຮອງຂໍ້ມູນ ເພື່ອຮັກສາຄວາມປອດໄພຂໍ້ມູນຂ່າວສານ ບໍ່ໃຫ້ເສຍຫາຍ;

6.3. ສຳຮອງຂໍ້ມູນໄວ້ໃນ ອຸປະກອນບັນທຶກຂໍ້ມູນ (External Hard disk) ເປັນປົກກະຕິ;

6.4. ກວດສອບຂໍ້ມູນທີ່ສຳຮອງແຕ່ 3 ຫາ 6 ເດືອນ ເພື່ອຮັບປະກັນຄວາມຖືກຕ້ອງ ແລະ ພ້ອມໃຊ້ງານຂອງຂໍ້ມູນ;

6.5. ກຳນົດແບບແຜນ ຫຼື ວິທີການ ກູ້ຂໍ້ມູນຄອມພິວເຕີຄືນຢ່າງສະໝ່ຳສະເໝີ (Data Recovery Capability) ໂດຍຕ້ອງສາມາດກູ້ຄືນໄດ້ທັນທີທີ່ລະບົບຫຼົ້ມ.

IV. ການຮັກສາສຸນຂໍ້ມູນຂ່າວສານ ໃຫ້ມີຄວາມປອດໄພ

1. ການຮັກສາຄວາມປອດໄພທາງກາຍະພາບ

ການຮັກສາຄວາມປອດໄພທາງກາຍະພາບ ຄວນປະຕິບັດໄດ້ດັ່ງນີ້:

1.1 ສຳລັບຜູ້ທີ່ມາພົວພັນວຽກງານກັບສຸນຂໍ້ມູນຂ່າວສານ ຕ້ອງມີການບັນທຶກລາຍຊື່, ວັນ ແລະ ເວລາການ ເຂົ້າ-ອອກ;

1.2 ການເຂົ້າ-ອອກ ຫ້ອງເຄື່ອງອຸປະກອນ ຕ້ອງຕິດຕັ້ງລະບົບກວດກາລາຍນິ້ວມື, ມີລະຫັດການ ເຂົ້າ-ອອກປະຕູສະເພາະ, ມີບັດປະຈຳຕົວສະແດງຕົວຕົນ ແລະ ຕິດຕັ້ງລະບົບກ້ອງວົງຈອນປິດໃນການຕິດຕາມ ແລະ ຮັກສາຄວາມປອດໄພ;

1.3 ວາງນະໂຍບາຍ ຫຼື ກົດລະບຽບສະເພາະໃນການບໍລິການລູກຄ້າຢ່າງເຂັ້ມງວດ;

1.4 ຈັດຫ້ອງເຕົ້ານົກສະເພາະໃຫ້ຜູ້ເຂົ້າມາໃຊ້ບໍລິການ ເພື່ອໃຫ້ສາມາດກວດກາ, ຕິດຕາມ ແລະ ສະດວກໃນການປັບປຸງລະບົບອຸປະກອນຂອງຕົນ;

1.5 ຕິດຕັ້ງສັນຍານເຕືອນໄພ ເພື່ອແຈ້ງເຕືອນເມື່ອມີເຫດການສຸກເສີນເກີດຂຶ້ນ;

1.6 ຄວນມີລະບົບໄຟຟ້າສຳຮອງອັດຕະໂນມັດ ເພື່ອຮັບປະກັນໃນເວລາໄຟຟ້າຂັດຂ້ອງ;

1.7 ອຸນຫະພູມໃນຫ້ອງເຄື່ອງອຸປະກອນຕ້ອງບໍ່ເກີນ 20-22 ອົງສາ;

1.8 ຄວນຕິດຕັ້ງລະບົບກວດຈັບຄວັນ ຫຼື ອາຍຄວາມຮ້ອນ ເພື່ອແຈ້ງເຕືອນເຫດທີ່ເກີດຂຶ້ນພາຍໃນຕຶກອາຄານ;

1.9 ກວດສອບລະບົບປ້ອງກັນໄພພາຍໃນສູນຂໍ້ມູນຂ່າວສານຢ່າງເປັນປົກກະຕິ ເພື່ອໃຫ້ມີຄວາມພ້ອມໃນການໃຊ້ງານ.

2. ການບຳລຸງຮັກສາອຸປະກອນຮາດແວ

ການຮັກສາເຄືອຂ່າຍຄອມພິວເຕີໃຫ້ມີຄວາມປອດໄພ ຄວນມີການບຳລຸງຮັກສາອຸປະກອນຮາດແວ, ກວດກາການປະຕິບັດການ ຫຼື ການທຳງານໃຫ້ຖືກວິທີ ດັ່ງນີ້:

2.1 ຂຶ້ນແຜນງົບປະມານ ໃນການຈັດຊື້ບັນດາອຸປະກອນຮາດແວ;

2.2 ຜູ້ໃຊ້ ຫຼື ຜູ້ຄຸ້ມຄອງເຄືອຂ່າຍຄອມພິວເຕີ ຕ້ອງໄດ້ກວດກາລະບົບອຸປະກອນຮາດແວທີ່ນຳໃຊ້ເຂົ້າໃນການຄຸ້ມຄອງເຄືອຂ່າຍຄອມພິວເຕີຂອງຕົນເປັນປະຈຳ ຖ້າຫາກມີຄວາມເສຍຫາຍ ຫຼື ໃກ້ໝົດອາຍຸການນຳໃຊ້ ຕ້ອງໄດ້ວາງແຜນປ່ຽນຖ່າຍໂດຍທັນທີ;

2.3 ລະບົບຄອມພິວເຕີ, ລະບົບຄອມພິວເຕີແມ່ຂ່າຍ, ອຸປະກອນເຊື່ອມຕໍ່ ແລະ ອຸປະກອນ ຮັບ-ສົ່ງ ສັນຍານ ຕ້ອງມີລະບົບໄຟຫຼໍ່ລ້ຽງສຳຮອງ (UPS) ເພື່ອຮັບປະກັນໃຫ້ລະບົບສາມາດໃຊ້ການໄດ້ຢ່າງຕໍ່ເນື່ອງ ໃນເວລາກະແສໄຟຕົກ ຫຼື ໄຟຟ້າມາບໍ່ປົກກະຕິ;

2.4 ທຳຄວາມສະອາດຄອມພິວເຕີໃຫ້ເປັນປະຈຳ ເພື່ອບໍ່ໃຫ້ມີຂີ້ຝຸ່ນ ເຊັ່ນ: ຫນ້າຈໍ, ແປ້ນພິມ, Mouse ແລະ Case Computer ເປັນຕົ້ນ.

3. ການບຳລຸງຮັກສາຊອບແວ

ການບຳລຸງຮັກສາລະບົບຄອມພິວເຕີແມ່ຂ່າຍ ແລະ ລະບົບຄອມພິວເຕີ ໃຫ້ມີຄວາມປອດໄພ ຄວນມີການກວດກາຕິດຕາມຊອບແວ ຫຼື ລະບົບປະຕິບັດການໃຫ້ຖືກວິທີ ດັ່ງນີ້:

3.1 ປັບປຸງລະບົບປະຕິບັດການຄອມພິວເຕີ ຢ່າງເປັນປົກກະຕິ;

3.2 ຕິດຕັ້ງ ແລະ ນຳໃຊ້ໂປແກຣມທີ່ໄດ້ຮັບອະນຸຍາດນຳໃຊ້ (Software License) ພ້ອມຕິດຕາມ ແລະ ກວດກາອັນໝົດອາຍຸການນຳໃຊ້;

3.3 ຈັດລຽງຂໍ້ມູນຮາດດິດ (Disk Defragment) ເພື່ອເພີ່ມຄວາມໄວການປະມວນຜົນຂໍ້ມູນ;

3.4 ລຶບໂປຣແກຣມຄອມພິວເຕີທີ່ບໍ່ໄດ້ໃຊ້ງານອອກ.

4. ການຮັກສາຄວາມປອດໄພຂໍ້ມູນເອເລັກໂຕຣນິກ

ການຮັກສາຂໍ້ມູນເອເລັກໂຕຣນິກ ໃຫ້ມີຄວາມປອດໄພ ຄວນຈັດລັນຄວາມປອດໄພຂໍ້ມູນເປັນແຕ່ລະລຳດັບ ດັ່ງນີ້:

4.1 ຈັດລຳດັບຄວາມສຳຄັນຂອງຂໍ້ມູນເອເລັກໂຕຣນິກ;

4.2 ເຂົ້າລະຫັດຂໍ້ມູນເອເລັກໂຕຣນິກ;

4.3 ກຳນົດສິດການເຂົ້າເຖິງຂໍ້ມູນເອເລັກໂຕຣນິກ;

4.4 ການຈັດເກັບຂໍ້ມູນເອເລັກໂຕຣນິກໄວ້ຫຼາຍບ່ອນ ຕ້ອງໃຫ້ມີປະລິມານ, ເນື້ອໃນ ຖືກຕ້ອງ ແລະ ຄືກັນ;

4.5 ນຳໃຊ້ຊອບແວລຶບຂໍ້ມູນ ແລະ ເຄື່ອງຈັກທຸບທຳລາຍ ໃນການທຳລາຍຂໍ້ມູນທີ່ບັນຈຸຢູ່ໃນອຸປະກອນບັນທຶກຂໍ້ມູນ ເຊັ່ນ: Harddisk, CD, DVD, Hard drive.

V. ການປະສານງານ ແລະ ການຮ່ວມມື

ການແກ້ໄຂເຫດສຸກເສີນທາງລະບົບຄອມພິວເຕີ ພາຍໃນສູນຂໍ້ມູນຂ່າວສານ ຄວນປະຕິບັດ ດັ່ງນີ້:

1. ສູນຂໍ້ມູນຂ່າວສານ ຕ້ອງສ້າງໜ່ວຍງານຮັກສາຄວາມປອດໄພທາງຄອມພິວເຕີຂອງຕົນສະເພາະ ເພື່ອເຮັດໜ້າທີ່ໃນການປະສານງານຮ່ວມມືກັບ ສູນສະກັດກັ້ນ ແລະ ແກ້ໄຂເຫດສຸກເສີນທາງຄອມພິວເຕີ (ສູນລາວເຊີດ) ໃນການປ້ອງກັນ ແລະ ແກ້ໄຂເຫດສຸກເສີນທາງໄຊເບີ;

2. ປະຕິບັດຕາມຂັ້ນຕອນ, ມາດຕະຖານເຕັກນິກວິຊາການ ໃນເວລາດຳເນີນການແກ້ໄຂເຫດສຸກເສີນທາງລະບົບຄອມພິວເຕີ;

3. ສ້າງ ແລະ ແຈ້ງທີ່ຢູ່, ເບີໂທລະສັບ ແລະ ອີເມວ ໃຫ້ການຈັດຕັ້ງທີ່ກ່ຽວຂ້ອງ ຫຼື ໜ່ວຍງານສະກັດກັ້ນ ແລະ ແກ້ໄຂເຫດສຸກເສີນທາງຄອມພິວເຕີ;

4. ຮ່ວມມືກັນຈັດຝຶກອົບຮົມວິຊາການ, ຝຶກແອບຕົວຈິງໃນການແກ້ໄຂ ແລະ ຮັບມືກັບເຫດສຸກເສີນທາງລະບົບຄອມພິວເຕີ.

VI. ການກວດກາຄວາມປອດໄພຂອງລະບົບຄອມພິວເຕີແມ່ຂ່າຍ ແລະ ເຄືອຂ່າຍຄອມພິວເຕີ

1. ການຕິດຕາມໄພຄຸກຄາມທາງລະບົບຄອມພິວເຕີ

ເພື່ອຮູ້ທັນ, ປ້ອງກັນ ແລະ ລະມັດລະວັງໄພຄຸກຄາມທາງລະບົບຄອມພິວເຕີ ຄວນປະຕິບັດ ດັ່ງນີ້:

1.1 ຜູ້ຄຸ້ມຄອງເຄືອຂ່າຍຄອມພິວເຕີ ແລະ ຜູ້ໃຊ້ຄອມພິວເຕີທົ່ວໄປ ຄວນຕິດຕາມຂໍ້ມູນຂ່າວສານ, ການແຈ້ງເຕືອນໄພ ແລະ ວິທີການຮັບມືໃນການປ້ອງກັນການແຮັກເວັບໄຊ, ການບຸກໂຈມຕີ ເຄືອຂ່າຍຄອມພິວເຕີ, ການແຜ່ລະບາດຂອງ ເມົ່າແວ ແລະ ອື່ນໆ;

1.2 ປະຕິບັດຕາມການແນະນຳວິທີການປ້ອງກັນ ແລະ ການແກ້ໄຂທາງວິຊາການ ຈາກໜ່ວຍງານຄຸ້ມຄອງຄວາມປອດໄພ ຫຼື ສູນສະກັດກັ້ນ ແລະ ແກ້ໄຂເຫດສຸກເສີນທາງຄອມພິວເຕີ ທີ່ໄດ້ອອກແຈ້ງເຕືອນ ເປັນແຕ່ລະໄລຍະ.

2. ການປະເມີນຄວາມສ່ຽງ

ເພື່ອປ້ອງກັນລະບົບຄອມພິວເຕີແມ່ຂ່າຍ ແລະ ເຄືອຂ່າຍຄອມພິວເຕີບໍ່ໃຫ້ເກີດຜົນເສຍຫາຍ ຜູ້ຄຸ້ມຄອງລະບົບດັ່ງກ່າວ ຄວນມີການປະເມີນຄວາມສ່ຽງ ຊຶ່ງສາມາດປະຕິບັດຕາມຂັ້ນຕອນ ດັ່ງນີ້:

2.1 ວິເຄາະ ການບຸກລຸກໂຈມຕີເຄືອຂ່າຍຄອມພິວເຕີ ທີ່ອາດເກີດຂຶ້ນ;

2.2 ປະເມີນຄວາມສ່ຽງຂອງອຸປະກອນທີ່ເຊື່ອມຕໍ່ເຂົ້າກັບເຄືອຂ່າຍຄອມພິວເຕີ;

2.3 ປະເມີນຄວາມສ່ຽງຂອງຜູ້ປະຕິບັດການ ອາດເກີດຂຶ້ນໄດ້ຈາກການດຳເນີນການ, ການຈັດລຳດັບຄວາມສຳຄັນໃນການເຂົ້າເຖິງຂໍ້ມູນ ຫຼື ການໃຫ້ບໍລິການ ການເຂົ້າເຖິງຂໍ້ມູນ;

2.4 ປະເມີນຄວາມສ່ຽງດ້ານເຕັກນິກ ອາດເກີດຂຶ້ນຈາກລະບົບຄອມພິວເຕີ, ເຄື່ອງມື ແລະ ອຸປະກອນຖືກໂຈມຕີຈາກໄວຣັດ, ໂປຣແກຣມຄອມພິວເຕີ ຫຼື ການຖືກເຈາະລະບົບຄອມພິວເຕີ;

2.5 ຄວາມສ່ຽງທີ່ອາດຈະເກີດຈາກໄພພິບັດທຳມະຊາດ ອາດເກີດຄວາມເສຍຫາຍກັບເຄືອຂ່າຍຄອມພິວເຕີ ເປັນຕົ້ນ ລະບົບຄອມພິວເຕີແມ່ຂ່າຍ ແລະ ເຄືອຂ່າຍຄອມພິວເຕີ ຢຸດທຳງານ ບໍ່ສາມາດສະໜອງຂໍ້ມູນຂ່າວສານໄດ້;

2.6 ປະເມີນຜົນກະທົບ ແລະ ຜົນເສຍຫາຍຕໍ່ອົງກອນ.

3. ການກວດສອບຄວາມປອດໄພ

ການກວດສອບຈຸດບົກຜ່ອງ ຫຼື ຊ່ອງໂຫວ່ທີ່ອາດຈະເກີດຂຶ້ນໃນລະບົບຄອມພິວເຕີແມ່ຂ່າຍ ແລະ ເຄືອຂ່າຍຄອມພິວເຕີ ຄວນປະຕິບັດ ດັ່ງນີ້:

3.1 ກວດກາຊ່ອງໂຫວ່ຂອງລະບົບຄອມພິວເຕີແມ່ຂ່າຍ ແລະ ເຄືອຂ່າຍຄອມພິວເຕີ ເພື່ອຊອກຫາຈຸດບົກຜ່ອງ, ວິທີການປັບປຸງ, ປ້ອງກັນ ແລະ ແກ້ໄຂ;

3.2 ທົດສອບການປະຕິບັດການຂອງ ລະບົບຄອມພິວເຕີແມ່ຂ່າຍ ແລະ ເຄືອຂ່າຍຄອມພິວເຕີຈາກພາຍໃນ ແລະ ພາຍນອກອົງກອນດ້ວຍວິທີການເຈາະ ຫຼື ຢຸດຕິການປະຕິບັດການ.

4. ການເຝົ້າລະວັງຄວາມປອດໄພ

ການເຝົ້າລະວັງຄວາມປອດໄພສູນຂໍ້ມູນຂ່າວສານ ຄວນປະຕິບັດ ດັ່ງນີ້:

4.1 ຕິດຕັ້ງລະບົບເຝົ້າລະວັງ, ຕິດຕາມ, ກວດກາການບຸກລຸກໂຈມຕີລະບົບຄອມພິວເຕີແມ່ຂ່າຍ ແລະ ເຄືອຂ່າຍຄອມພິວເຕີ;

4.2 ຈັດຕັ້ງການເຝົ້າລະວັງຕິດຕາມ, ກວດກາການບຸກລຸກໂຈມຕີລະບົບຄອມພິວເຕີແມ່ຂ່າຍ ແລະ ເຄືອຂ່າຍຄອມພິວເຕີ 24/7 ຊົ່ວໂມງ.

VII. ການຈັດຕັ້ງປະຕິບັດ

ມອບໃຫ້ ສູນສະກັດກັ້ນ ແລະ ແກ້ໄຂເຫດສຸກເສີນທາງລະບົບຄອມພິວເຕີ ປະສານສົມທົບກັບພາກສ່ວນທີ່ກ່ຽວຂ້ອງ ແລະ ອົງການປົກຄອງທ້ອງຖິ່ນ ຈັດຕັ້ງໂຄສະນາ, ເຜີຍແຜ່, ແນະນຳ ແລະ ປະຕິບັດ ຄຳແນະນຳສະບັບນີ້ໃຫ້ໄດ້ຮັບຜົນດີ.

ບັນດາກະຊວງ, ອົງການທຽບເທົ່າກະຊວງ ແລະ ອົງການປົກຄອງທ້ອງຖິ່ນ, ບຸກຄົນ, ນິຕິບຸກຄົນ ພາຍໃນ ສປປ ລາວ ຈົ່ງຮັບຮູ້ ແລະ ນຳໄປຈັດຕັ້ງປະຕິບັດໃຫ້ຖືກຕ້ອງ.

VIII. ຜົນສັກສິດ

ຄຳແນະນຳສະບັບນີ້ ມີຜົນສັກສິດນັບແຕ່ວັນລົງລາຍເຊັນເປັນຕົ້ນໄປ ແລະ ຈັດຕັ້ງປະຕິບັດພາຍຫຼັງທີ່ໄດ້ລົງໃນຈົດໝາຍເຫດທາງລັດຖະການ ສິບຫ້າວັນ.

ລັດຖະມົນຕີ

ປອ. ທັນສະໄໝ ກົມມະສິດ