ສາທາລະນະລັດ ປະຊາທິປະໄຕ ປະຊາຊົນລາວ
ສັນຕິພາບ ເອກະລາດ ປະຊາທິປະໄຕ ເອກະພາບ ວັດທະນະຖາວອນ

ທະນາຄານແຫ່ງ ສປປ ລາວ

ເລກທີ 696 /ທຫລ
ນະຄອນຫຼວງວຽງຈັນ, ວັນທີ 06 ທັນວາ 2021

ຂໍ້ຕົກລົງ
ວ່າດ້ວຍການບໍລິຫານລະບົບເຕັກໂນໂລຊີຂໍ້ມູນຂ່າວສານ ຂອງຜູ້ໃຫ້ບໍລິການທາງດ້ານການເງິນ

- ອີງຕາມ ກົດໝາຍວ່າດ້ວຍທະນາຄານແຫ່ງ ສປປ ລາວ (ສະບັບປັບປຸງ) ເລກທີ 47/ສພຊ, ລົງວັນທີ 19 ມິຖຸນາ 2018;
- ອີງຕາມ ດຳລັດວ່າດ້ວຍການຈັດຕັ້ງ ແລະ ການເຄື່ອນໄຫວ ຂອງທະນາຄານແຫ່ງ ສປປ ລາວ ເລກທີ 196/ ສພຊ, ລົງວັນທີ 24 ມິຖຸນາ 2016;
- ອີງຕາມການຄົ້ນຄວ້າ ແລະ ນຳສະເໜີ ຂອງກົມເຕັກໂນໂລຊີຂໍ້ມູນຂ່າວສານ.

ຜູ້ວ່າການທະນາຄານແຫ່ງ ສປປ ລາວ ຕົກລົງ:

ໝວດທີ 1
ບົດບັນຍັດທົ່ວໄປ

ມາດຕາ 1 ຈຸດປະສົງ

ຂໍ້ຕົກລົງສະບັບນີ້ ກຳນົດຫຼັກການກ່ຽວກັບການບໍລິຫານລະບົບເຕັກໂນໂລຊີຂໍ້ມູນຂ່າວສານຂອງຜູ້ໃຫ້ບໍລິການທາງດ້ານການເງິນ ເພື່ອໃຫ້ມີຄວາມປອດໄພ, ໜ້າເຊື່ອຖື ແລະ ພ້ອມໃຊ້ງານ ແນໃສ່ເຮັດໃຫ້ການບໍລິການທາງດ້ານການເງິນ ມີປະສິດທິພາບ ແລະ ຮັບປະກັນການເຊື່ອມໂຍງກັບລະບົບຕ່າງໆຂອງທະນາຄານແຫ່ງ ສປປ ລາວ ໄດ້ຢ່າງມີປະສິດທິຜົນ.

ມາດຕາ 2 ການບໍລິຫານລະບົບເຕັກໂນໂລຊີຂໍ້ມູນຂ່າວສານຂອງຜູ້ໃຫ້ບໍລິການທາງດ້ານການເງິນ

ການບໍລິຫານລະບົບເຕັກໂນໂລຊີຂໍ້ມູນຂ່າວສານຂອງຜູ້ໃຫ້ບໍລິການທາງດ້ານການເງິນ ແມ່ນຂະບວນການປະມວນຜົນກ່ຽວກັບການນຳໃຊ້ລະບົບໂປຣແກຣມນຳໃຊ້, ການບໍລິຫານຄວາມສ່ຽງ, ການຮັກສາຄວາມປອດໄພ ຂອງລະບົບເຕັກໂນໂລຊີຂໍ້ມູນຂ່າວສານ ຊຶ່ງຜູ້ໃຫ້ບໍລິການທາງດ້ານການເງິນ ຕ້ອງວາງແຜນ ແລະ ກຳນົດກົນໄກການດຳເນີນງານຂອງລະບົບດັ່ງກ່າວ ໃຫ້ມີຄວາມໜ້າເຊື່ອຖື ແລະ ມີຄວາມພ້ອມໃນການນຳໃຊ້ຕະຫຼອດເວລາ.

ມາດຕາ 3 ການອະທິບາຍຄຳສັບ

ຄຳສັບທີ່ນຳໃຊ້ໃນຂໍ້ຕົກລົງສະບັບນີ້ ມີຄວາມໝາຍ ດັ່ງນີ້:

1. **ຜູ້ໃຫ້ບໍລິການທາງດ້ານການເງິນ** ໝາຍເຖິງ ທະນາຄານທຸລະກິດ, ສະຖາບັນການເງິນຈຸລະພາກທີ່ຮັບເງິນຝາກ, ສະຖາບັນການເງິນຈຸລະພາກທີ່ບໍ່ຮັບເງິນຝາກ, ສະຫະກອນສິນເຊື່ອ ແລະ ເງິນຝາກປະຢັດ, ບໍລິສັດເຊົ່າສິນເຊື່ອ, ໂຮງຊວດຈຳ ແລະ ຜູ້ໃຫ້ບໍລິການທາງດ້ານການເງິນອື່ນ ທີ່ຢູ່ພາຍໃຕ້ການຄຸ້ມຄອງຂອງທະນາຄານແຫ່ງ ສປປ ລາວ;

2. **ການເຊື່ອມໂຍງກັບລະບົບຕ່າງໆຂອງທະນາຄານແຫ່ງ ສປປ ລາວ** ໝາຍເຖິງ ການເຊື່ອມຕໍ່ ຫຼື ເປັນສະມາຊິກ ເພື່ອເຂົ້າມານຳໃຊ້ລະບົບຕ່າງໆຂອງທະນາຄານແຫ່ງ ສປປ ລາວ ເຊັ່ນ: ລະບົບ LAPASS, LAPNET, MIS, CIB;

3. **ລະບົບການເຊື່ອມຕໍ່ໂປຣແກຣມ** (Application Programming Interface:API) ໝາຍເຖິງ ຊຸດຄຳສັ່ງຂອງໂປຣແກຣມ ທີ່ເຮັດໜ້າທີ່ເປັນຊ່ອງທາງໃນການແລກປ່ຽນຂໍ້ມູນລະຫວ່າງລະບົບໂປຣແກຣມນຳໃຊ້ໜຶ່ງ ໄປຫາລະບົບໂປຣແກຣມນຳໃຊ້ອື່ນ;

4. **ມັລແວ (Malware)** ໝາຍເຖິງ ຊຸດຄຳສັ່ງຄອມພິວເຕີທີ່ສ້າງຂຶ້ນ ເພື່ອທຳລາຍ ຫຼື ໂຈລະກຳຂໍ້ມູນ ໃນລະບົບຄອມພິວເຕີ;

5. **ໄຟຣ໌ວໍ (Firewall)** ໝາຍເຖິງ ອຸປະກອນຮັກສາຄວາມປອດໄພ ຊຶ່ງເຮັດໜ້າທີ່ກວດກາ ແລະ ກັ່ນຕອງຂໍ້ມູນທີ່ຜ່ານເຂົ້າ - ອອກ ລະບົບເຄືອຂ່າຍ;

6. **ເຣົາເຕີ (Router)** ໝາຍເຖິງ ອຸປະກອນເຊື່ອມຕໍ່ເຄືອຂ່າຍລະຫວ່າງອົງກອນຫາອົງກອນ ຊຶ່ງເຮັດໜ້າທີ່ເຊື່ອມຕໍ່ລະບົບເຄືອຂ່າຍເຂົ້າຫາກັນ, ຈັດຫາເສັ້ນທາງທີ່ດີທີ່ສຸດເພື່ອຮັບ - ສົ່ງຂໍ້ມູນຜ່ານລະບົບເຄືອຂ່າຍ, ເປັນຕົວກາງໃນການສົ່ງຕໍ່ຂໍ້ມູນໄປຫາເຄືອຂ່າຍອື່ນ ແລະ ປ້ອງກັນຂໍ້ມູນໂດຍມີການເຂົ້າລະຫັດການຮັບ - ສົ່ງຂໍ້ມູນຈາກຕົ້ນທາງຫາປາຍທາງ;

7. **ອຸປະກອນກວດກາ ແລະ ດັກຈັບຜູ້ບຸກລຸກ (Intrusion Prevention System/ Intrusion Detection Prevention System)** ໝາຍເຖິງ ເຕັກໂນໂລຊີທີ່ເຮັດໜ້າທີ່ ກວດກາ, ດັກຈັບ, ກັ່ນຕອງ ແລະ ປ້ອງກັນການບຸກລຸກ ເຂົ້າມາໃນລະບົບເຄືອຂ່າຍ ແລະ ແຈ້ງເຕືອນໄພໃຫ້ກັບຜູ້ຄຸ້ມຄອງລະບົບໄດ້ຮັບຊາບ;

8. **ລະບົບການຕິດຕາມການນຳໃຊ້ (Network Monitoring)** ໝາຍເຖິງ ລະບົບທີ່ຕິດຕາມສະຖານະຂອງອຸປະກອນເຄືອຂ່າຍ, ແຈ້ງເຕືອນໃນກໍລະນີເກີດຂໍ້ຜິດພາດກັບອຸປະກອນ, ກວດກາປະສິດທິພາບການເຮັດວຽກຂອງລະບົບເຄືອຂ່າຍ ແລະ ອຸປະກອນທີ່ກ່ຽວຂ້ອງ, ກວດສອບປະລິມານການໃຊ້ງານຊັບພະຍາກອນຂອງລະບົບເຄືອຂ່າຍ ແລະ ເຝົ້າລະວັງແນວໂນ້ມທີ່ອາດຈະເປັນໄພຄຸກຄາມຕໍ່ລະບົບເຄືອຂ່າຍ;

9. **ລະບົບບໍລິຫານການນຳໃຊ້ຊັບພະຍາກອນພາຍໃນເຄືອຂ່າຍແບບລວມສຸນ (Domain Controler)** ໝາຍເຖິງ ລະບົບທີ່ເຮັດໜ້າທີ່ຕິດຕາມການໃຊ້ງານຂອງຜູ້ໃຊ້, ຝ່າຍເອກະສານ ແລະ ອຸປະກອນ

ການພົມຕ່າງໆພາຍໃນເຄືອຂ່າຍ ເພື່ອຢັ້ງຢືນການເຂົ້າໃຊ້ລະບົບ ແລະ ໃຫ້ສິດຜູ້ໃຊ້ສາມາດເຂົ້າເຖິງຊັບພະຍາກອນພາຍໃນອົງກອນໄດ້;

10. **ລະບົບໜ່ວຍແມ່ຂ່າຍແບບຈຳລອງ (Virtualizations)** ໝາຍເຖິງ ການຈຳລອງຊັບພະຍາກອນຈິງຂອງລະບົບຄອມພິວເຕີ ໂດຍມີການລວບລວມຊັບພະຍາກອນດ້ານ ການປະມວນຜົນ, ການຈັດເກັບຂໍ້ມູນ ແລະ ການຕິດຕໍ່ສື່ສານໃນແຕ່ລະອຸປະກອນມາລວມກັນໄວ້ທີ່ສູນກາງ. ຈາກນັ້ນ, ຈຶ່ງສາມາດນຳໃຊ້ຊັບພະຍາກອນເຫຼົ່ານັ້ນ ໄປຈັດສັນການໃຊ້ປະໂຫຍດໄດ້ຕາມຄວາມເໝາະສົມ ຫຼື ຕາມຄວາມຕ້ອງການຂອງແຕ່ລະລະບົບ;

11. **ອຸປະກອນເອເລັກໂຕຣນິກ (Internet of Things)** ໝາຍເຖິງ ວັດຖຸສິ່ງຂອງທີ່ສາມາດເຊື່ອມຕໍ່, ຄວບຄຸມ ແລະ ສົ່ງຂໍ້ມູນຫາກັນໄດ້ ໂດຍຜ່ານລະບົບເຄືອຂ່າຍພາຍໃນ ແລະ ອິນເຕີເນັດ ເຊັ່ນ: Smart phone, Smart Home, Smart TV, Smart printer;

12. **HA (High Availability)** ໝາຍເຖິງ ອົງປະກອບຂອງລະບົບເຕັກໂນໂລຊີຂໍ້ມູນຂ່າວສານ ທີ່ອອກແບບ ເພື່ອຮັບປະກັນການດຳເນີນການໃຫ້ບໍລິການຢ່າງຕໍ່ເນື່ອງ;

13. **RTO (Recovery Time Objectives)** ໝາຍເຖິງ ໄລຍະເວລາກູ້ຄືນລະບົບທີ່ຍອມຮັບໄດ້ ໂດຍການກຳນົດຂອບເຂດໄລຍະເວລາສູງສຸດທີ່ຍອມຮັບໄດ້;

14. **RPO (Recovery Point Objectives)** ໝາຍເຖິງ ປະລິມານຂໍ້ມູນເສຍຫາຍໃນເວລາທີ່ຍອມຮັບໄດ້ ເປັນການກຳນົດເວລາທີ່ຂໍ້ມູນນັ້ນ ຕ້ອງໄດ້ຮັບການກູ້ຄືນຈາກໜ່ວຍຈັດເກັບສຳຮອງຂໍ້ມູນ ເພື່ອໃຫ້ກັບຄືນສູ່ການປະຕິບັດງານຕາມປົກກະຕິ;

15. **ເຫດການຜິດປົກກະຕິ** ໝາຍເຖິງ ເຫດການແຈ້ງເຕືອນໄພຕ່າງໆທີ່ອາດຈະເກີດຂຶ້ນຕໍ່ລະບົບ ເຊັ່ນ: ການແຈ້ງເຕືອນການເຮັດວຽກທີ່ຜິດປົກກະຕິຂອງໜ່ວຍແມ່ຂ່າຍ (ໄຟສີຂຽວ ຫຼື ສົ້ມ), ພຶດຕິກຳການເຂົ້ານຳໃຊ້ລະບົບເຄືອຂ່າຍທີ່ຜິດປົກກະຕິທີ່ເຮັດໃຫ້ການເຮັດວຽກຂອງຄວາມຈຳຊົ່ວຄາວ ແລະ ໜ່ວຍປະມວນຜົນເຮັດວຽກສູງເກີນກຳນົດ;

16. **ເຫດການສຸກເສີນ** ໝາຍເຖິງ ເຫດການທີ່ສົ່ງຜົນກະທົບຕໍ່ລະບົບເຕັກໂນໂລຊີຂໍ້ມູນຂ່າວສານໃນທາງລົບ ເຮັດໃຫ້ບໍ່ສາມາດເຮັດວຽກໄດ້ ນັບແຕ່ລະດັບເບົາໄປຫາໜັກ ເຊັ່ນ: ບັນຫາການເຮັດວຽກຂອງໜ່ວຍເກັບຂໍ້ມູນ, ໜ່ວຍແມ່ຂ່າຍ ຫຼື ລະບົບໂຄງລ່າງພື້ນຖານເສຍຫາຍ, ການຢຸດສະຫງັກຂອງການຈ່າຍໄຟຟ້າ, ການເກີດອັກຄີໄພ, ອຸທົກກະໄພ ແລະ ເຫດການກໍ່ການຮ້າຍຕ່າງໆ ຕາມລຳດັບ.

ມາດຕາ 4 ຂອບເຂດການນຳໃຊ້

ຂໍ້ຕົກລົງສະບັບນີ້ ນຳໃຊ້ສຳລັບຜູ້ໃຫ້ບໍລິການທາງດ້ານການເງິນ ທີ່ມີລະບົບເຕັກໂນໂລຊີຂໍ້ມູນຂ່າວສານເປັນຂອງຕົນເອງ ຫຼື ນຳໃຊ້ລະບົບເຕັກໂນໂລຊີຂໍ້ມູນຂ່າວສານຈາກພາຍນອກ ທີ່ຢູ່ພາຍໃນປະເທດ ຫຼື ຕ່າງປະເທດ ລວມທັງການນຳໃຊ້ລະບົບເຕັກໂນໂລຊີຂໍ້ມູນຂ່າວສານແບບປະສົມປະສານ.

ໝວດທີ 2
ລະບົບໂປຣແກຣມນຳໃຊ້ເຂົ້າໃນລະບົບເຕັກໂນໂລຊີຂໍ້ມູນຂ່າວສານ

ມາດຕາ 5 ລະບົບໂປຣແກຣມນຳໃຊ້

ລະບົບໂປຣແກຣມນຳໃຊ້ ແມ່ນ ຊຸດຄຳສັ່ງ ຫຼື ໂປຣແກຣມ ທີ່ຍັນຊາຄອມພິວເຕີ ແລະ ອຸປະກອນເອເລັກໂຕຣນິກ ເຊັ່ນ: ລະບົບໂປຣແກຣມການຊຳລະ ແລະ ຫັກບັນຊີຂອງ ສປປ ລາວ (Lao Payment and Settlement System: LaPASS), ລະບົບໂປຣແກຣມບໍລິຫານຂໍ້ມູນທາງການເງິນຂອງທະນາຄານທຸລະກິດ (Managemet Information System: MIS), ໂປຣແກຣມບັນຊີຂອງທະນາຄານແຫ່ງ ສປປ ລາວ ແລະ ອື່ນໆ.

ມາດຕາ 6 ການພັດທະນາລະບົບໂປຣແກຣມນຳໃຊ້

ຜູ້ໃຫ້ບໍລິການທາງດ້ານການເງິນ ຕ້ອງມີບົດສຶກສາຄວາມຕ້ອງການທາງດ້ານວຽກງານ, ບົດສຶກສາຄວາມເປັນໄປໄດ້ທາງດ້ານເຕັກນິກ, ບົດປະເມີນການຈັດຕັ້ງປະຕິບັດ ແລະ ແຜນທົດລອງລະບົບກ່ອນການນຳໃຊ້ຕົວຈິງ ເພື່ອຢັ້ງຢືນຄວາມຖືກຕ້ອງ, ຄົບຖ້ວນ ແລະ ສອດຄ່ອງກັບວຽກງານ.

ມາດຕາ 7 ລະບົບໂປຣແກຣມນຳໃຊ້ຈາກພາຍນອກ

ຜູ້ໃຫ້ບໍລິການທາງດ້ານການເງິນ ທີ່ໃຊ້ບໍລິການລະບົບໂປຣແກຣມນຳໃຊ້ຈາກພາຍນອກ ຕ້ອງມີມາດຕະການປ້ອງກັນຄວາມສ່ຽງທາງດ້ານການຮົ່ວໄຫຼຂອງຂໍ້ມູນ, ການແອບແຝງເມັ່ງແວ (Malware), ໄວຣັສ ແລະ ອື່ນໆ ດ້ວຍການເລືອກເຟັ້ນຜູ້ໃຫ້ບໍລິການທີ່ມີຄວາມໜ້າເຊື່ອຖື, ມີວິທີການກວດກາ ແລະ ທົດສອບຈຸດບົກຜ່ອງ ກ່ອນການນຳໃຊ້ຕົວຈິງ ເພື່ອຄວາມໝັ້ນຄົງ ແລະ ປອດໄພ.

ມາດຕາ 8 ການເຊື່ອມຕໍ່ລະບົບໂປຣແກຣມນຳໃຊ້

ຜູ້ໃຫ້ບໍລິການທາງດ້ານການເງິນ ຕ້ອງກຳນົດມາດຕະຖານການເຊື່ອມຕໍ່ລະບົບໂປຣແກຣມນຳໃຊ້ຂອງຕົນ ໃຫ້ເປັນໄປຕາມມາດຕະຖານການເຊື່ອມຕໍ່ (API-Application Programming Interface) ທີ່ກຳນົດໄວ້ ຮັບປະກັນການເຊື່ອມໂຍງ ແລະ ສະໜອງຂໍ້ມູນກັບລະບົບຕ່າງໆຂອງທະນາຄານແຫ່ງ ສປປ ລາວ ພ້ອມທັງ ວິເຄາະປະເມີນຄວາມສ່ຽງກ່ອນການເຊື່ອມຕໍ່ລະບົບ ແລະ ກຳນົດຂອບເຂດການແລກປ່ຽນຂໍ້ມູນສະເພາະທີ່ນຳໃຊ້ຕົວຈິງ.

ໝວດທີ 3
ການບໍລິຫານຄວາມສ່ຽງຂອງລະບົບເຕັກໂນໂລຊີຂໍ້ມູນຂ່າວສານ

ມາດຕາ 9 ຄວາມສ່ຽງດ້ານລະບົບເຕັກໂນໂລຊີຂໍ້ມູນຂ່າວສານ

ຄວາມສ່ຽງດ້ານລະບົບເຕັກໂນໂລຊີຂໍ້ມູນຂ່າວສານ ແມ່ນເຫດການຕ່າງໆທີ່ເປັນຜົນກະທົບທາງລົບຕໍ່ຂໍ້ມູນທາງດ້ານທຸລະກິດ, ລະບົບທີ່ມີຄວາມສຳຄັນຕໍ່ການດຳເນີນທຸລະກິດ ແລະ ຂັ້ນຕອນໃນການດຳເນີນທຸລະກິດ.

ມາດຕາ 10 ຄວາມສ່ຽງດ້ານບໍລິຫານ

ຜູ້ໃຫ້ບໍລິການທາງດ້ານການເງິນ ຕ້ອງກຳນົດມາດຕະຖານເງື່ອນໄຂຂອງພະນັກງານທີ່ເຮັດວຽກງານບໍລິຫານຄວາມສ່ຽງ ຊຶ່ງຕ້ອງມີຜູ້ບໍລິຫານ ແລະ ບຸກຄະລາກອນທີ່ມີຄວາມຮູ້ຄວາມສາມາດ ໃນການບໍລິຫານຄວາມສ່ຽງດ້ານລະບົບເຕັກໂນໂລຊີຂໍ້ມູນຂ່າວສານ.

ມາດຕາ 11 ການຕິດຕາມ, ການປະເມີນ ແລະ ການລາຍງານຄວາມສ່ຽງຂອງລະບົບ

ຜູ້ໃຫ້ບໍລິການທາງດ້ານການເງິນ ຕ້ອງຕິດຕາມ, ປະເມີນ ແລະ ລາຍງານ ຄວາມສ່ຽງດ້ານລະບົບເຕັກໂນໂລຊີຂໍ້ມູນຂ່າວສານ ໂດຍກຳນົດວິທີການ ແລະ ຂັ້ນຕອນ ຜ່ານຂະບວນການ ລະບຸ, ວິເຄາະ ແລະ ຈັດລຳດັບຄວາມສ່ຽງ.

ໝວດທີ 4
ການຮັກສາຄວາມປອດໄພຂອງລະບົບເຕັກໂນໂລຊີຂໍ້ມູນຂ່າວສານ

ມາດຕາ 12 ຄວາມປອດໄພດ້ານຂໍ້ມູນ

ຜູ້ໃຫ້ບໍລິການທາງດ້ານການເງິນ ຕ້ອງມີວິທີການປ້ອງກັນຂໍ້ມູນເສຍຫາຍ (Data Loss Prevention), ການເຂົ້າເຖິງຄອມພິວເຕີ ແລະ ຂໍ້ມູນໂດຍບໍ່ໄດ້ຮັບອະນຸຍາດ (Unauthorised Access), ການເຂົ້າປອມແປງຂໍ້ມູນ (Data Modification) ແລະ ການສຳເນົາຂໍ້ມູນ (Data Copying).

ມາດຕາ 13 ຄວາມປອດໄພດ້ານເຄືອຂ່າຍ

ຜູ້ໃຫ້ບໍລິການທາງດ້ານການເງິນ ຕ້ອງມີລະບົບເຄືອຂ່າຍທີ່ປະກອບດ້ວຍ ອຸປະກອນຮັກສາຄວາມປອດໄພ (Firewall), ອຸປະກອນເຊື່ອມຕໍ່ເຄືອຂ່າຍລະຫວ່າງອົງກອນຫາອົງກອນ (Router), ອຸປະກອນກວດກາ ແລະ ດັກຈັບຜູ້ບຸກລຸກ (IPS/IDS), ລະບົບກວດກາ-ປ້ອງກັນໄວຣັສ, ລະບົບການຕິດຕາມການນຳໃຊ້ອຸປະກອນເຄືອຂ່າຍ (Network Monitoring). ສຳລັບ ຄອມພິວເຕີທີ່ຈະເຊື່ອມຕໍ່ເຂົ້າລະບົບເຄືອຂ່າຍ ຕ້ອງຜ່ານລະບົບບໍລິຫານການນຳໃຊ້ຊັບພະຍາກອນແບບລວມສຸນ (Domain Controler), ພ້ອມນັ້ນ ລະບົບເຄືອຂ່າຍຕ້ອງມີການຈຳກັດການເຊື່ອມຕໍ່ຂອງບັນດາອຸປະກອນເອເລັກໂຕຣນິກ.

ມາດຕາ 14 ຄວາມປອດໄພດ້ານລະບົບໜ່ວຍແມ່ຂ່າຍ

ຜູ້ໃຫ້ບໍລິການທາງດ້ານການເງິນ ຕ້ອງມີການກຳນົດສິດການເຂົ້ານຳໃຊ້, ຍົກລະດັບລະບົບປະຕິບັດການ, ທົບທວນ ແລະ ກວດກາການຕັ້ງຄ່າລະບົບໜ່ວຍແມ່ຂ່າຍ ຢ່າງເປັນປະຈຳ ເພື່ອຮັບປະກັນ ແລະ ຫຼຸດຜ່ອນຄວາມສ່ຽງການຖືກໂຈມຕີຈາກພາຍນອກ. ພ້ອມນັ້ນ ຕ້ອງມີລະບົບໂປຣແກຣມ ເພື່ອຕິດຕາມກວດກາ, ແຈ້ງເຕືອນ ແລະ ລາຍງານການເຂົ້າອອກ ແລະ ບັນດາເຫດການຜິດປົກກະຕິທີ່ເກີດຂຶ້ນໃນລະບົບ. ໃນກໍລະນີ ທີ່ມີການນຳໃຊ້ລະບົບໜ່ວຍແມ່ຂ່າຍແບບຈຳລອງ (Virtualizations) ຕ້ອງມີການຄຸ້ມຄອງລະບົບຝ່າຍຈຳລອງໃຫ້ມີຄວາມປອດໄພ.

ມາດຕາ 15 ຄວາມປອດໄພດ້ານໂປຣແກຣມນຳໃຊ້

ຜູ້ໃຫ້ບໍລິການທາງດ້ານການເງິນ ຕ້ອງກວດກາດ້ານຄວາມປອດໄພ ກ່ຽວກັບຊຸດຄຳສັ່ງໂປຣແກຣມນຳໃຊ້ຂອງຕົນ (Source code) ພ້ອມທັງມີການທົບທວນປັບປຸງຄວາມປອດໄພກ່ຽວກັບຊຸດຄຳສັ່ງໂປຣແກຣມນຳໃຊ້ ໃຫ້ສອດຄ່ອງກັບການປ່ຽນແປງແຕ່ລະໄລຍະ ເພື່ອຫຼຸດຜ່ອນຊ່ອງຫວ່າງຕ່າງໆ ທີ່ສາມາດພາໃຫ້ເກີດຄວາມສ່ຽງຕໍ່ລະບົບໂປຣແກຣມນຳໃຊ້.

ມາດຕາ 16 ການແລກປ່ຽນຂໍ້ມູນດ້ານຄວາມປອດໄພ

ຜູ້ໃຫ້ບໍລິການທາງດ້ານການເງິນ ຕ້ອງມີການແລກປ່ຽນຂໍ້ມູນຄວາມປອດໄພທາງດ້ານລະບົບເຕັກໂນໂລຊີຂໍ້ມູນຂ່າວສານ ກັບພາກສ່ວນອື່ນ ແລະ ມີການຮ່ວມມືກັນໃນການຮັບມືກັບການໂຈມຕີທາງດ້ານເຕັກໂນໂລຊີຂໍ້ມູນຂ່າວສານ.

ໝວດທີ 5
ຄວາມໜ້າເຊື່ອຖືຂອງລະບົບເຕັກໂນໂລຊີຂໍ້ມູນຂ່າວສານ

ມາດຕາ 17 ຄວາມໜ້າເຊື່ອຖືດ້ານຂໍ້ມູນ

ຜູ້ໃຫ້ບໍລິການທາງດ້ານການເງິນ ຕ້ອງມີການເຂົ້າລະຫັດຂໍ້ມູນ, ການຢັ້ງຢືນຕົວຕົນ, ການບໍລິຫານການເຂົ້າເຖິງຂໍ້ມູນ ແລະ ການຕິດຕາມການເຂົ້າເຖິງຂໍ້ມູນ ເພື່ອຮັກສາຄວາມຖືກຕ້ອງ, ຄົບຖ້ວນ ແລະ ສົມບູນຂອງຂໍ້ມູນ ນັບແຕ່ວັນທີ່ລະບົບຖືກ ສ້າງຂຶ້ນ, ເກັບຮັກສາໄວ້ ແລະ ຈົນຮອດວັນຖືກທຳລາຍ.

ມາດຕາ 18 ຄວາມໜ້າເຊື່ອຖືດ້ານເຄືອຂ່າຍ ແລະ ໜ່ວຍແມ່ຂ່າຍ

ຜູ້ໃຫ້ບໍລິການທາງດ້ານການເງິນ ຕ້ອງອອກແບບລະບົບເຄືອຂ່າຍ ແລະ ໜ່ວຍແມ່ຂ່າຍເປັນໄປຕາມມາດຕະຖານທີ່ມີຄວາມໜ້າເຊື່ອຖື, ລະບົບເຄືອຂ່າຍ ແລະ ໜ່ວຍແມ່ຂ່າຍ ຕ້ອງຖືກເກັບຮັກສາໄວ້ໃນສູນຂໍ້ມູນຫຼັກ ແລະ ສູນສຳຮອງຂໍ້ມູນ ທີ່ເປັນໄປຕາມມາດຕະຖານຄວາມປອດໄພດ້ານຕ່າງໆ ແລະ ສອດຄ່ອງກັບຄວາມຕ້ອງການດ້ານທຸລະກິດ, ອຸປະກອນເຄືອຂ່າຍ ແລະ ໜ່ວຍແມ່ຂ່າຍ ຕ້ອງມີການອັບເດດຊອບແວ ຢ່າງເປັນປະຈຳ, ລະບົບຈຳລອງທີ່ນຳໃຊ້ຕ້ອງມີລາຍເຊັນ, ມີລະບົບປ້ອງກັນໄວຣັສ, ມີການທົດລອງຍ້າຍການປະຕິບັດງານຈາກສູນຂໍ້ມູນຫຼັກໄປສູນສຳຮອງຂໍ້ມູນ ຢ່າງໜ້ອຍ ໜຶ່ງ ຄັ້ງຕໍ່ປີ, ມີການທົດລອງເຈາະລະບົບ ເພື່ອຊອກຫາຈຸດບົກຜ່ອງທາງດ້ານເຄືອຂ່າຍ ແລະ ໜ່ວຍແມ່ຂ່າຍ ພ້ອມທັງມີແຜນການຟື້ນຟູລະບົບເຄືອຂ່າຍ.

ມາດຕາ 19 ຄວາມໜ້າເຊື່ອຖືດ້ານໂປຣແກຣມນຳໃຊ້

ຜູ້ໃຫ້ບໍລິການທາງດ້ານການເງິນ ຕ້ອງນຳໃຊ້ ຫຼື ພັດທະນາໂປຣແກຣມທີ່ເປັນໄປຕາມມາດຕະຖານທີ່ມີຄວາມໜ້າເຊື່ອຖືທາງດ້ານການພັດທະນາໂປຣແກຣມນຳໃຊ້ ແລະ ມີຄວາມສອດຄ່ອງຕາມຄວາມຕ້ອງການທາງດ້ານທຸລະກິດ.

ໝວດທີ 6
ການຮັບປະກັນຄວາມພ້ອມໃຊ້ງານຂອງລະບົບເຕັກໂນໂລຊີຂໍ້ມູນຂ່າວສານ

ມາດຕາ 20 ການຮັບປະກັນຄວາມພ້ອມໃຊ້ງານ

ລະບົບເຕັກໂນໂລຊີຂໍ້ມູນຂ່າວສານຂອງຜູ້ໃຫ້ບໍລິການທາງດ້ານການເງິນ ຕ້ອງອອກແບບໃຫ້ເໝາະສົມກັບການເຄື່ອນໄຫວຂອງວຽກງານ ເພື່ອຮັບປະກັນຄວາມພ້ອມໃນການດຳເນີນງານ ໂດຍການອອກແບບໃຫ້ເປັນລະບົບທີ່ມີຄວາມຕໍ່ເນື່ອງ (high availability: HA). ການຮັບປະກັນພ້ອມໃຊ້ງານຂອງລະບົບເຕັກໂນໂລຊີຂໍ້ມູນຂ່າວສານ ຕ້ອງທົບທວນຢ່າງເປັນປະຈຳ ເພື່ອຫາຈຸດອ່ອນທີ່ຄວນປັບປຸງແກ້ໄຂກ່ອນເກີດບັນຫາຂຶ້ນຕົວຈິງ.

ຜູ້ໃຫ້ບໍລິການທາງດ້ານການເງິນ ຕ້ອງມີແບບແຜນຕິດຕາມກວດກາ ການຕັ້ງຄ່າ, ການປ່ຽນຖ່າຍ ແລະ ການຍົກລະດັບຂອງລະບົບໃນແຕ່ລະໄລຍະ ເພື່ອຮັບປະກັນຄວາມພ້ອມໃຊ້ງານ ແລະ ຫຼີກລ້ຽງການເກີດມີບັນຫາຂັດຂ້ອງຂອງລະບົບ ແລະ ທັນກັບສະພາບການ.

ມາດຕາ 21 ການບໍລິຫານເຫດການຜິດປົກກະຕິ

ຜູ້ໃຫ້ບໍລິການທາງດ້ານການເງິນ ຕ້ອງມີແບບແຜນການບໍລິຫານເຫດການຜິດປົກກະຕິ ດ້ານລະບົບເຕັກໂນໂລຊີຂໍ້ມູນຂ່າວສານ ຊຶ່ງລວມເຖິງເຫດການຜິດປົກກະຕິຈາກໄພຄຸກຄາມທາງລະບົບຄອມພິວເຕີຢ່າງເໝາະສົມ, ທັນສະພາບການ ແລະ ສາມາດແກ້ໄຂໃຫ້ກັບສູ່ສະພາບປົກກະຕິຢ່າງວ່ອງໄວ ເພື່ອຫຼຸດຜ່ອນຄວາມເສຍຫາຍຕໍ່ທຸລະກິດຂອງຜູ້ໃຫ້ບໍລິການທາງດ້ານການເງິນ, ມີການກຳນົດວິທີການບໍລິຫານເຫດການຜິດປົກກະຕິ ນັບຕັ້ງແຕ່ຂັ້ນຕອນການບັນທຶກເຫດການ, ກຳນົດລະດັບຄວາມຮຸນແຮງ, ການວິເຄາະສາເຫດ, ປະເມີນຜົນກະທົບ, ການແກ້ໄຂ ແລະ ລາຍງານ ຊຶ່ງຕ້ອງມີການຕິດຕາມກວດກາລະບົບ ແລະ ເຝົ້າລະວັງໄພຄຸກຄາມ ໂດຍມີເຄື່ອງມືໃນການກວດຈັບເຫດການຜິດປົກກະຕິ ຫຼື ໄພຄຸກຄາມຕ່າງໆ ເພື່ອສາມາດປ້ອງກັນ ແລະ ຮັບມືໄດ້ຢ່າງທັນການ. ນອກຈາກນີ້, ຕ້ອງມີການແຈ້ງເຕືອນເຫດການຜິດປົກກະຕິໃຫ້ແກ່ພາກສ່ວນທີ່ກ່ຽວຂ້ອງຮັບຊາບ.

ມາດຕາ 22 ແຜນສຸກເສີນ ແລະ ການຟື້ນຟູລະບົບ

ຜູ້ໃຫ້ບໍລິການທາງດ້ານການເງິນ ຕ້ອງສ້າງແຜນສຸກເສີນ ເພື່ອສາມາດຮັບມືກັບເຫດການຂັດຂ້ອງ ຫຼື ແກ້ໄຂທາງດ້ານເຕັກນິກຕ່າງໆທີ່ອາດຈະເກີດຂຶ້ນ ຊຶ່ງແຜນດັ່ງກ່າວຕ້ອງຖືກຮັບຮອງໂດຍຄະນະຜູ້ບໍລິຫານ. ນອກຈາກນັ້ນ, ຍັງຕ້ອງມີຄູ່ມືໃນການຈັດຕັ້ງປະຕິບັດ ພ້ອມທັງທົບທວນຄືນ ແລະ ທົດລອງການຈັດຕັ້ງປະຕິບັດແຜນສຸກເສີນ ຢ່າງໜ້ອຍ ປີລະຄັ້ງ. ພ້ອມກັນນັ້ນ, ຜູ້ໃຫ້ບໍລິການທາງດ້ານການເງິນ ຕ້ອງສ້າງແຜນການຟື້ນຟູລະບົບ ທີ່ປະກອບມີ ການກຳນົດ RTO (Recovery Time Objectives) ແລະ RPO (Recovery Point Objectives) ເພື່ອໃຫ້ມີຜົນກະທົບໜ້ອຍທີ່ສຸດ. ຂະບວນການຟື້ນຟູລະບົບ ຕ້ອງປະຕິບັດຕາມແຜນສຸກເສີນທີ່ກຳນົດໄວ້, ກໍລະນີເຫັນວ່າ ເກີດເຫດການນອກເໜືອແຜນທີ່ກຳນົດ ຕ້ອງກຳນົດວິທີການຟື້ນຟູເພີ່ມເຕີມ ແລະ ຖືກຮັບຮອງໂດຍຄະນະຜູ້ບໍລິຫານ ກ່ອນຈັດຕັ້ງປະຕິບັດ. ພາຍຫຼັງການຟື້ນຟູລະບົບສຳເລັດ ຕ້ອງບັນທຶກລາຍລະອຽດ ແລະ ປັບປຸງເຂົ້າໃນແຜນສຸກເສີນ.

ໝວດທີ 7
ບົດບັນຍັດສຸດທ້າຍ

ມາດຕາ 23 ການຈັດຕັ້ງປະຕິບັດ

ກົມເຕັກໂນໂລຊີຂໍ້ມູນຂ່າວສານ, ບັນດາກົມ ແລະ ທຽບເທົ່າກົມ ຂອງທະນາຄານແຫ່ງ ສປປ ລາວ ທີ່ກ່ຽວຂ້ອງ ເປັນຜູ້ຕິດຕາມ ແລະ ຈັດຕັ້ງປະຕິບັດ ຂໍ້ຕົກລົງສະບັບນີ້ ຕາມພາລະບົດໜ້າທີ່ຂອງຕົນ.

ຜູ້ໃຫ້ບໍລິການທາງດ້ານການເງິນ ທີ່ຢູ່ພາຍໃຕ້ການຄຸ້ມຄອງຂອງທະນາຄານແຫ່ງ ສປປ ລາວ ຈົ່ງຮັບຮູ້ ແລະ ຈັດຕັ້ງປະຕິບັດ ຂໍ້ຕົກລົງສະບັບນີ້ ຢ່າງເຂັ້ມງວດ

ມາດຕາ 24 ຜົນສັກສິດ

ຂໍ້ຕົກລົງສະບັບນີ້ ມີຜົນສັກສິດ ນັບແຕ່ວັນລົງລາຍເຊັນເປັນຕົ້ນໄປ.

ຂໍ້ກຳນົດ ຫຼື ບົດບັນຍັດໃດ ທີ່ຂັດກັບຂໍ້ຕົກລົງສະບັບນີ້ ລ້ວນແຕ່ຖືກຍົກເລີກ.

ຜູ້ວ່າການທະນາຄານ ແຫ່ງ ສປປ ລາວ

ສອນໄຊ ສິດພະໄຊ