



ສາທາລະນະລັດ ປະຊາທິປະໄຕ ປະຊາຊົນລາວ
ສັນຕິພາບ ເອກະລາດ ປະຊາທິປະໄຕ ເອກະພາບ ວັດທະນະຖາວອນ

ກະຊວງໄປສະນີ, ໂທລະຄົມມະນາຄົມ ແລະ ການສື່ສານ

ເລກທີ 2543 /ປທສ
ນະຄອນຫຼວງວຽງຈັນ, ວັນທີ 24 ກັນຍາ 2018

ຄໍາແນະນໍາ

ການຈັດຕັ້ງປະຕິບັດ ກົດໝາຍວ່າດ້ວຍ ການຕ້ານ ແລະ ສະກັດກັ້ນອາຊະຍາກຳທາງລະບົບຄອມພິວເຕີ

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

ລັດຖະມົນຕີ ອອກຄໍາແນະນໍາ:

I. ຈຸດປະສົງ

ຄໍາແນະນໍາສະບັບນີ້ ຜັນຂະຫຍາຍ ແລະ ແນະນໍາການຈັດຕັ້ງປະຕິບັດ ເນື້ອໃນບາງມາດຕາຂອງກົດໝາຍວ່າດ້ວຍ ການຕ້ານ ແລະ ສະກັດກັ້ນອາຊະຍາກຳທາງລະບົບຄອມພິວເຕີ, ສະບັບເລກທີ 61/ສພຊ, ລົງວັນທີ 15 ກໍລະກົດ 2015 ເພື່ອເຮັດໃຫ້ເນື້ອໃນຂອງກົດໝາຍດັ່ງກ່າວ ມີຄວາມລະອຽດ ແລະ ຈະແຈ້ງຂຶ້ນຕື່ມ ໂດຍການອະທິບາຍເພີ່ມຕື່ມບັນດາ ເນື້ອໃນທີ່ມີລັກສະນະເຕັກນິກວິຊາການ, ພຶດຕິກຳທີ່ເປັນອາຊະຍາກຳທາງລະບົບຄອມພິວເຕີ ພ້ອມທັງຍົກຕົວຢ່າງ ປະກອບໃຫ້ເຂົ້າໃຈໄດ້ງ່າຍໃນການນຳໃຊ້ ແນໃສ່ເຮັດໃຫ້ການຈັດຕັ້ງປະຕິບັດກົດໝາຍໃຫ້ຖືກຕ້ອງ, ມີປະສິດທິພາບ, ປະສິດທິຜົນ ແລະ ມີຄວາມເປັນເອກະພາບໃນຂອບເຂດທົ່ວປະເທດ.

II. ອະທິບາຍເພີ່ມຕື່ມເນື້ອໃນຄໍາສັບບາງມາດຕາ

1. ມາດຕາ 9 ການເປີດເຜີຍມາດຕະການປ້ອງກັນການເຂົ້າເຖິງລະບົບຄອມພິວເຕີ ແມ່ນ ການນຳເອົາມາດຕະການປ້ອງກັນສະເພາະ ໄປເປີດເຜີຍໂດຍບໍ່ໄດ້ຮັບອະນຸຍາດ ເຊັ່ນ: ລະຫັດຜ່ານ, ຊ່ອງໂຫ້ວ, ວິທີການເຈາະ, ວິທີການໂຈມຕີ ລະບົບຄອມພິວເຕີ ແລະ ວິທີການອື່ນ ທີ່ກໍ່ໃຫ້ເກີດຄວາມເສັຍຫາຍ ຕໍ່ລັດ, ບຸກຄົນ, ນິຕິບຸກຄົນ, ການຈັດຕັ້ງ ແລະ ສັງຄົມ.

ຕົວຢ່າງ: ທ້າວ ກໍ ໄດ້ນຳເອົາລະຫັດຜ່ານ, ຊ່ອງໂຫ້ວ, ວິທີການເຈາະ ແລະ ວິທີການໂຈມຕີ ລະບົບຄອມພິວເຕີ ຂອງອົງກອນໃດໜຶ່ງໄປເປີດເຜີຍຕໍ່ບຸກຄົນອື່ນ ໂດຍບໍ່ໄດ້ຮັບອະນຸຍາດ ຊຶ່ງເຮັດໃຫ້ລະບົບຄອມພິວເຕີຂອງອົງກອນດັ່ງກ່າວ ເກີດຄວາມເສັຍຫາຍ. ✓

2. ມາດຕາ 10 ການເຂົ້າເຖິງລະບົບຄອມພິວເຕີ ໂດຍບໍ່ໄດ້ຮັບອະນຸຍາດ ແມ່ນ ການນຳໃຊ້ອຸປະກອນ ຫຼື ເຄື່ອງມື ເອເລັກໂຕຣນິກ ເຊັ່ນ: ໂປຣແກຣມຄອມພິວເຕີ, ໂປຣແກຣມປະສົງຮ້າຍ, ອຸປະກອນບັນທຶກຂໍ້ມູນ ແລະ ວິທີການອື່ນ ໃນການເຂົ້າເຖິງລະບົບຄອມພິວເຕີ ທີ່ມີມາດຕະການປ້ອງກັນສະເພາະ ເພື່ອລັກເອົາຂໍ້ມູນທາງດ້ານການຄ້າ, ດ້ານການ ເງິນ, ຄວາມລັບ ແລະ ຂໍ້ມູນອື່ນໆ ຂອງບຸກຄົນ, ນິຕິບຸກຄົນ, ການຈັດຕັ້ງ.

ຕົວຢ່າງ: ທ້າວ ກໍ ໄດ້ນຳໃຊ້ອຸປະກອນບັນທຶກຂໍ້ມູນທີ່ມີໄວຣັດເຊື່ອມຕໍ່ກັບລະບົບຄອມພິວເຕີ ຂອງອົງກອນໃດ ໜຶ່ງ ໂດຍບໍ່ໄດ້ຮັບອະນຸຍາດ ເພື່ອລັກເອົາຂໍ້ມູນ, ປອມແປງຂໍ້ມູນ, ປ່ຽນແປງຂໍ້ມູນ ຫຼື ກະທຳການອື່ນ ຊຶ່ງເຮັດໃຫ້ລະບົບ ຄອມພິວເຕີຂອງອົງກອນດັ່ງກ່າວ ເກີດຄວາມເສັຍຫາຍ.

3. ມາດຕາ 11 ການຕັດຕໍ່ເນື້ອໃນ, ຮູບ, ພາບເຄື່ອນໄຫວ, ສຽງ ແລະ ວິດີໂອ ໂດຍບໍ່ໄດ້ຮັບອະນຸຍາດ ບໍ່ວ່າຈະ ເປັນ ການສ້າງຂຶ້ນໃໝ່, ການເພີ່ມເຕີມ ຫຼື ການດັດແປງຈາກຕົ້ນສະບັບ ດ້ວຍວິທີການທາງເອເລັກໂຕຣນິກ ຫຼື ວິທີການ ອື່ນ ເຊັ່ນ: ໂປຣແກຣມຕັດຕໍ່ ຮູບ, ພາບເຄື່ອນໄຫວ, ສຽງ ແລະ ວິດີໂອ ນຳໄປເຜີຍແຜ່ ຜ່ານລະບົບຄອມພິວເຕີ ເຊັ່ນ: ສື່ ສັງຄົມອອນລາຍ, ເວັບໄຊ ແລະ ຜ່ານທາງອື່ນ ຊຶ່ງສ້າງຄວາມເສັຍຫາຍໃຫ້ແກ່ ບຸກຄົນ, ນິຕິບຸກຄົນ ແລະ ການຈັດຕັ້ງທີ່ ກ່ຽວຂ້ອງ.

ຕົວຢ່າງ: ທ້າວ ກໍ ໄດ້ນຳເອົາຮູບ ຂອງນາງ ຂໍ ໂດຍບໍ່ໄດ້ຮັບອະນຸຍາດ ມາຕັດຕໍ່, ດັດແປງ, ແກ້ໄຂ ດ້ວຍການນຳ ໃຊ້ ໂປຣແກຣມ Photoshop ແລະ ນຳເອົາຮູບດັ່ງກ່າວໄປເຜີຍແຜ່ຜ່ານທາງ Facebook ຊຶ່ງສ້າງຄວາມເສັຍຫາຍ ແລະ ເສັຍຫາຍໃຫ້ແກ່ນາງ ຂໍ.

4. ມາດຕາ 12 ການລັດເອົາຂໍ້ມູນໃນລະບົບຄອມພິວເຕີ ໂດຍບໍ່ໄດ້ຮັບອະນຸຍາດ ແມ່ນ ການດັກເອົາຂໍ້ມູນທີ່ ກຳລັງຮັບ ຫຼື ສົ່ງ ຜ່ານລະບົບຄອມພິວເຕີ ເຊັ່ນ: ການດັກເອົາຂໍ້ມູນຜ່ານທາງ ຈົດໝາຍເອເລັກໂຕຣນິກ (Email), ການ ໂທລະສັບ, ການສົນທະນາທາງຂໍ້ຄວາມ ແລະ ຮູບແບບອື່ນ ດ້ວຍການນຳໃຊ້ເຄື່ອງມືທາງດ້ານເອເລັກໂຕຣນິກ.

ຕົວຢ່າງ: ທ້າວ ກໍ ໄດ້ສົ່ງຈົດໝາຍເອເລັກໂຕຣນິກຫາ ທ້າວ ຂໍ ວ່າຈະໂອນເງິນຄ່າສິນຄ້າໄປໃຫ້ຈຳນວນໜຶ່ງຕື້ກີບ ໂດຍຈະສົ່ງເຂົ້າບັນຊີຂອງ ທ້າວ ຂໍ ແຕ່ ທ້າວ ຄໍ ໄດ້ນຳໃຊ້ເຄື່ອງມືເອເລັກໂຕຣນິກລັດດັກຈັບເອົາຂໍ້ມູນການສົນທະນາ ລະຫວ່າງ ທ້າວ ກໍ ແລະ ທ້າວ ຂໍ ຊຶ່ງຂໍ້ມູນດັ່ງກ່າວອາດສ້າງຄວາມເສັຍຫາຍໃຫ້ແກ່ ທ້າວ ກໍ ແລະ ທ້າວ ຂໍ ໄດ້.

5. ມາດຕາ 13 ການສ້າງຄວາມເສັຍຫາຍຜ່ານສື່ສັງຄົມອອນລາຍ ແມ່ນ ສະແດງອອກດ້ວຍການກະທຳ ດັ່ງນີ້:

ຕົວຢ່າງ 1: ທ້າວ ກໍ ເອົາຂໍ້ມູນທີ່ມີລັກສະນະ ໃສ່ຮ້າຍປ້າຍສີ, ໜິ້ນປະໝາດ, ໃຊ້ຄຳສັບບໍ່ສຸພາບ ເຜີຍແຜ່ລົງ ເຟສ ບຸກ (Facebook), ວ່ອດແອັບ (WhatsApp), ລາຍ (LINE), ທະວິດເຕີ (Twitter), ຢູທູບ (Youtube) ແລະ ຜ່ານ ທາງອື່ນ;

ຕົວຢ່າງ 2: ທ້າວ ກໍ ນຳເອົາຂໍ້ມູນ ທີ່ມີລັກສະນະໃຊ້ຄວາມຮຸນແຮງ, ຂໍ້ມູນເທັດ, ຂໍ້ມູນຫຼອກລວງ, ຂໍ້ມູນທີ່ບໍ່ ເປັນຄວາມຈິງ ເຜີຍແຜ່ລົງ ເຟສບຸກ (Facebook), ວ່ອດແອັບ (WhatsApp), ລາຍ (LINE), ທະວິດເຕີ (Twitter), ຢູທູບ (Youtube) ແລະ ຜ່ານທາງອື່ນ;

ຕົວຢ່າງ 3: ທ້າວ ກໍ ນຳເອົາຂໍ້ມູນ ທີ່ເປັນການທຳລາຍຄວາມໝັ້ນຄົງຂອງຊາດ, ຄວາມສະຫງົບ, ຄວາມເປັນ ລະບຽບຮຽບຮ້ອຍຂອງສັງຄົມ, ວັດທະນະທຳ ແລະ ຮິດຄອງປະເພນີອັນດີງາມຂອງຊາດ ເຜີຍແຜ່ລົງ ເຟສບຸກ (Facebook), ວ່ອດແອັບ (WhatsApp), ລາຍ (LINE), ທະວິດເຕີ (Twitter), ຢູທູບ (Youtube) ແລະ ຜ່ານ ທາງອື່ນ; ✓

ຕົວຢ່າງ 4: ທ້າວ ກໍ ນໍາເອົາຂໍ້ມູນ ທີ່ມີລັກສະນະຊວນເຊື້ອ, ບຸຍົງ ແລະ ສິ່ງເສີມ ປະຊາຊົນຕໍ່ຕ້ານ ລັດຖະບານ ຫຼື ແບ່ງແຍກຄວາມສາມັກຄີ ເຜີຍແຜ່ລົງ ເຟສບຸກ (Facebook), ວ່ອດແອັບ (WhatsApp), ລາຍ (LINE), ທະວິດເຕີ (Twitter), ຢູທູບ (Youtube) ແລະ ຜ່ານທາງອື່ນ;

ຕົວຢ່າງ 5: ທ້າວ ກໍ ໂຄສະນາຄ້າຂາຍຢາເສບຕິດ, ອາວຸດເສິກ, ອາວຸດເຄມີ, ຄ້າມະນຸດ, ຄ້າປະເວນີ, ຄ້າໂສເພນີ ແລະ ສິ່ງທີ່ຜິດກົດໝາຍ ເຜີຍແຜ່ລົງ ເຟສບຸກ (Facebook), ວ່ອດແອັບ (WhatsApp), ລາຍ (LINE), ທະວິດເຕີ (Twitter), ຢູທູບ (Youtube) ແລະ ຜ່ານທາງອື່ນ;

ຕົວຢ່າງ 6: ທ້າວ ກໍ ເຜີຍແຜ່ ຫຼື ສົ່ງຕໍ່ຂໍ້ມູນ ຕາມທີ່ໄດ້ກຳນົດໄວ້ໃນມາດຕາ 11 ແລະ 14 ຂອງກົດ ໝາຍວ່າ ດ້ວຍ ການຕ້ານ ແລະ ສະກັດກັ້ນອາຊະຍາກຳທາງລະບົບຄອມພິວເຕີ ລວມທັງ 1, 2, 3, 4 ແລະ ຂໍ້ 5 ຂອງມາດຕາ 13.

6. ມາດຕາ 14 ການເຜີຍແຜ່ສິ່ງລາມົກຜ່ານລະບົບຄອມພິວເຕີ ແມ່ນ ການຊື້ຂາຍ, ການແຈກຢາຍ, ການສົ່ງຕໍ່, ການແນະນຳ ແລະ ການເຜີຍແຜ່ຂໍ້ມູນທີ່ມີເນື້ອໃນສະແດງອອກຢ່າງຈະແຈ້ງເປັນຕົ້ນ ຮຸບ, ພາບເຄື່ອນໄຫວ, ສຽງ ແລະ ວິດີໂອ ກ່ຽວກັບອະໄວຍະວະເພດ ແລະ ພຶດຕິກຳທາງເພດຂອງຄົນ.

7. ມາດຕາ 15 ການລົບກວນລະບົບຄອມພິວເຕີ ແມ່ນ ການກະທຳ ດັ່ງນີ້:

7.1. ການນຳໃຊ້ໂປຣແກຣມຄອມພິວເຕີ, ໄວຣັດ ຫຼື ເຄື່ອງມືອື່ນ ເພື່ອຂັດຂວາງ ຫຼື ທຳລາຍ ການປະຕິບັດງານ ຂອງລະບົບຄອມພິວເຕີ.

ຕົວຢ່າງ: ທ້າວ ກໍ ໄດ້ໂຈມຕີ ລະບົບຄອມພິວເຕີ ຂອງອົງກອນໃດໜຶ່ງ ດ້ວຍວິທີການສົ່ງບໍລິມາດຂໍ້ມູນຈຳນວນ ຫຼວງຫຼາຍ (DDoS Attack) ເພື່ອຂັດຂວາງ ຫຼື ເຮັດໃຫ້ການປະຕິບັດງານ ຂອງລະບົບຄອມພິວເຕີ ທຳການບໍ່ເປັນ ປົກກະຕິ ຫຼື ບໍ່ສາມາດນຳໃຊ້ໄດ້ ຫຼື ການໂຈມຕີດ້ວຍການນຳໃຊ້ໄວຣັດ ເພື່ອລຶບ ແລະ ທຳລາຍ ພາຍຂໍ້ມູນສຳຄັນຕ່າງໆ ໃນລະບົບຄອມພິວເຕີ ຊຶ່ງເຮັດໃຫ້ອົງກອນດັ່ງກ່າວເກີດຄວາມເສັຍຫາຍ;

7.2. ການສົ່ງຂໍ້ມູນລະບົບຄອມພິວເຕີ ຫຼື ຈົດໝາຍທາງເອເລັກໂຕຣນິກ ໂດຍມີການປົກປິດທີ່ຢູ່ ຫຼື ແຫຼ່ງທີ່ມາ ຂອງຜູ້ສົ່ງ ເຊັ່ນ: ການສົ່ງຈົດໝາຍເອເລັກໂຕຣນິກປອມ, ການສົ່ງຂໍ້ຄວາມໂຄສະນາຊວນເຊື້ອ ແລະ ຮຸບແບບອື່ນ ເພື່ອ ລົບກວນ ແລະ/ຫຼື ທຳລາຍການປະຕິບັດງານຂອງລະບົບຄອມພິວເຕີ.

ຕົວຢ່າງ: ທ້າວ ກໍ ໄດ້ປອມໝາຍເລກທີ່ຢູ່ທາງອິນເຕີເນັດ (IP Address) ແລະ ສົ່ງອີເມວຈຳນວນຫຼວງຫຼາຍໄປ ຫານາງ ຂໍ ໂດຍປົກປິດແຫຼ່ງທີ່ມາ ຊຶ່ງລົບກວນການປະຕິບັດງານລະບົບຄອມພິວເຕີ ຂອງ ນາງ ຂໍ ຈົນເກີດມີການ ປະມວນຜົນຊັກຊ້າ ຫຼື ເສັຍຫາຍ ເຮັດໃຫ້ຄອມພິວເຕີ ເປ່ເພ.

8. ມາດຕາ 16 ການປອມແປງຂໍ້ມູນຄອມພິວເຕີ ແມ່ນ ການໃຊ້ຄອມພິວເຕີ ຫຼື ລະບົບຄອມພິວເຕີ ແລະ ອຸປະກອນເອເລັກໂຕຣນິກ ເພື່ອປ່ຽນແປງຂໍ້ມູນຄອມພິວເຕີ ດ້ວຍການກະທຳ ດັ່ງນີ້:

ຕົວຢ່າງ 1: ທ້າວ ກໍ ໄດ້ລັກເຂົ້າເຖິງລະບົບຄອມພິວເຕີ ຂອງວິທະຍາໄລໃດໜຶ່ງ ໂດຍມີຈຸດປະສົງ ປ້ອນຂໍ້ມູນ, ປ່ຽນແປງຂໍ້ມູນ, ລຶບຂໍ້ມູນ ການສຶກສາຂອງຕົນ ຫຼື ບຸກຄົນອື່ນ ເຊັ່ນ: ຄະແນນສອບເສັງ (ຈາກຄະແນນ 0 ມາເປັນ 9), ຄະແນນສະເລ່ຍ (F ມາເປັນ A), ປະຫວັດການຂຶ້ນຫ້ອງຮຽນ (ຈາກຂາດຮຽນຫຼາຍຊົ່ວໂມງ ເປັນ ການມາຮຽນ ປົກກະຕິ) ແລະ ຂໍ້ມູນອື່ນ; ✓

ຕົວຢ່າງ 2: ທ້າວ ກໍ ໄດ້ລັກເຂົ້າລະບົບຄອມພິວເຕີ ຂອງທະນາຄານໃດໜຶ່ງ ເພື່ອປ້ອນ ແລະ ປ່ຽນແປງຂໍ້ມູນທຸລະກຳທາງການເງິນ, ການຄ້າ ແລະ ຄວາມລັບ ເຊັ່ນ: ການປ່ຽນແປງ ຍອດເງິນໃນບັນຊີ, ການຊໍາລະເງິນຂອງລູກຄ້າ, ຂໍ້ມູນການໂອນເງິນ ຫຼື ປອມແປງເອກະສານເອເລັກໂຕຣນິກທີ່ເປັນຄວາມລັບຂອງທະນາຄານ ແລະ ຂໍ້ມູນອື່ນ;

ຕົວຢ່າງ 3: ທ້າວ ກໍ ໄດ້ສ້າງເວັບໄຊປອມ ຂອງທະນາຄານໃດໜຶ່ງ ເຊັ່ນ: ເວັບໄຊທະນາຄານແທ້ ແມ່ນ www.123abc-bank.la ມາເປັນເວັບໄຊປອມ www.123cba-bank.la ມີຈຸດປະສົງຫຼອກລວງ ຫຼື ຕົວະຍົວະບຸກຄົນອື່ນ ເພື່ອເອົາຂໍ້ມູນບັນຊີເງິນຝາກ, ລະຫັດບັດເຄຣດິດ, ລະຫັດນຳໃຊ້ອິນເຕີເນັດ ແລະ ຂໍ້ມູນອື່ນ.

9. ມາດຕາ 17 ການທຳລາຍຂໍ້ມູນຄອມພິວເຕີ ແມ່ນ ການລຶບ, ການດັດແກ້ ແລະ/ຫຼື ການປ່ຽນແປງ ຂໍ້ມູນຄອມພິວເຕີ ຫຼື ຂໍ້ມູນໃນລະບົບຄອມພິວເຕີ ເພື່ອເຮັດໃຫ້ຂໍ້ມູນ ຫຼື ລະບົບຄອມພິວເຕີ ນັ້ນເສັຍຫາຍ ແລະ ຜິດແປກຈາກຂໍ້ມູນເດີມ.

ຕົວຢ່າງ: ທ້າວ ກໍ ລັກເຂົ້າລະບົບຄອມພິວເຕີ ຂອງບໍລິສັດໃດໜຶ່ງ ເພື່ອລຶບ ຫຼື ທຳລາຍຂໍ້ມູນການເງິນ, ຂໍ້ມູນລູກຄ້າ, ຂໍ້ມູນໂຄງການ ແລະ ຂໍ້ມູນທີ່ສຳຄັນອື່ນ ຂອງບໍລິສັດອອກຈາກລະບົບຄອມພິວເຕີ ຊຶ່ງເຮັດໃຫ້ຂໍ້ມູນຂອງບໍລິສັດດັ່ງກ່າວຖືກທຳລາຍ ແລະ ເສັຍຫາຍ.

10. ມາດຕາ 18 ການດຳເນີນກິດຈະການ ກ່ຽວກັບເຄື່ອງມືກໍ່ອາຊະຍາກຳທາງລະບົບຄອມພິວເຕີ ແມ່ນ ການສ້າງໂປຣແກຣມໃໝ່ສະເພາະ, ການຜະລິດ, ການນຳເຂົ້າ, ການມີໄວ້ຄອບຄອງ, ການຊື້ຂາຍ, ການຈຳໜ່າຍ, ການໂຄສະນາເຜີຍແຜ່ ຫຼື ການແນະນຳ ເຄື່ອງມືດັ່ງກ່າວ ເປັນຕົ້ນໂປຣແກຣມຄອມພິວເຕີ ຫຼື ການອອກແບບຂໍ້ມູນຄອມພິວເຕີ ເພື່ອກໍ່ອາຊະຍາກຳທາງລະບົບຄອມພິວເຕີ.

ຕົວຢ່າງ: ທ້າວ ກໍ ໄດ້ດຳເນີນກິດຈະການກ່ຽວກັບ ເຄື່ອງມືຕັດສັນຍານ, ເຄື່ອງມືຄວບຄຸມການສື່ສານ, ການດັກຟັງ, ການລັດເອົາຂໍ້ມູນ, ການປອມແປງ ແລະ ປ່ຽນແປງຂໍ້ມູນຈາລະຈອນ, ການຈັບຈຸດພິກັດ, ເຄື່ອງມືເຈາະເຂົ້າຂໍ້ມູນຄອມພິວເຕີ ແລະ ອື່ນໆ ເພື່ອກໍ່ອາຊະຍາກຳທາງລະບົບຄອມພິວເຕີ.

11. ມາດຕາ 20 ການແຈ້ງເຕືອນແມ່ນ ກະຊວງໄປສະນີ, ໂທລະຄົມມະນາຄົມ ແລະ ການສື່ສານ ເປັນຜູ້ແຈ້ງໄພອັນຕະລາຍ ທີ່ເກີດຂຶ້ນໃນລະບົບຄອມພິວເຕີ ແລະ ອິນເຕີເນັດ ເປັນຕົ້ນ ການແຈ້ງເຕືອນເວັບໄຊປອມ, ໂປຣແກຣມປະສົງຮ້າຍ, ການແຈ້ງຊ່ອງໂຫວ່ຂອງລະບົບຄອມພິວເຕີ, ການຕົວະຍົວະທາງຈິດໝາຍເອເລັກໂຕຣນິກ ແລະ ອື່ນໆ.

ໃນກໍລະນີຫາກພົບເຫັນໄວຣັດ ທີ່ກຳລັງແຜ່ກະຈາຍ ໃນບໍລິສັດ ກໍ ຢູ່ຕ່າງປະເທດ ກະຊວງໄປສະນີ, ໂທລະຄົມມະນາຄົມ ແລະ ການສື່ສານ ຕ້ອງອອກແຈ້ງເຕືອນ ພ້ອມທັງແນະນຳວິທີການປ້ອງກັນໄວຣັດດັ່ງກ່າວ ເພື່ອໃຫ້ຜູ້ຄຸ້ມຄອງ ແລະ ຜູ້ຊົມໃຊ້ລະບົບຄອມພິວເຕີ ພາຍໃນປະເທດ ຮັບຊາບ.

ຜູ້ໃຫ້ບໍລິການລະບົບຄອມພິວເຕີ ຕ້ອງແຈ້ງເຕືອນ ແລະ ກຳນົດເງື່ອນໄຂ ໃນການເຂົ້າຫາລະບົບຄອມພິວເຕີ ເພື່ອຈຳກັດ ຫຼື ບໍ່ອະນຸຍາດໃຫ້ຜູ້ໃຊ້ບໍລິການບາງປະເພດ ເຂົ້າຫາລະບົບຄອມພິວເຕີ.

ຕົວຢ່າງ: ບໍລິສັດ ຂໍ ຊຶ່ງເປັນຜູ້ຄຸ້ມຄອງລະບົບຄອມພິວເຕີ ໄດ້ຮັບແຈ້ງເຕືອນ ກ່ຽວກັບການແຜ່ກະຈາຍຂອງໄວຣັດ Wanna Cry ຕ້ອງອອກແຈ້ງເຕືອນ ພ້ອມທັງແນະນຳວິທີການປ້ອງກັນໄວຣັດດັ່ງກ່າວ ໃຫ້ຜູ້ຊົມໃຊ້ລະບົບຄອມພິວເຕີ ຮັບຊາບ. ✓

12. ມາດຕາ 21 ການໃຫ້ຄໍາປຶກສາ ແມ່ນຂະແໜງການໄປສະນີ, ໂທລະຄົມມະນາຄົມ ແລະ ການສື່ສານ ເປັນຜູ້ໃຫ້ຄໍາປຶກສາ, ແນະນຳວິທີການປ້ອງກັນ ແລະ ການແກ້ໄຂທາງດ້ານເຕັກນິກ ເປັນຕົ້ນ: ການຊອກຫາແຫຼ່ງທີ່ມາຂອງການໂຈມຕີລະບົບຄອມພິວເຕີ, ການພິສູດຫຼັກຖານທາງເອເລັກໂຕຣນິກ, ການແກ້ໄຂຊ່ອງໂຫວ່ຂອງລະບົບຄອມພິວເຕີ, ການແກ້ໄຂປະກົດການຫຍ້ໍ້ທີ່ຜ່ານສື່ສັງຄົມອອນລາຍ ລວມເຖິງການໃຫ້ຄໍາປຶກສາກ່ຽວກັບວຽກງານຕ້ານ ແລະ ສະກັດກັ້ນອາຊະຍາກຳທາງລະບົບຄອມພິວເຕີ ແກ່ ບຸກຄົນ, ນິຕິບຸກຄົນ ແລະ ການຈັດຕັ້ງ ເພື່ອຫຼຸດຜ່ອນການສູນເສຍຂໍ້ມູນ, ການລົບກວນຂໍ້ມູນ, ບໍ່ໃຫ້ມີການຢຸດຕິການທ່າງານຂອງລະບົບຄອມພິວເຕີ, ສະກັດກັ້ນການກະຈາຍໄວຮັດຄອມພິວເຕີ ແລະ ການເຂົ້າທຳລາຍຂໍ້ມູນໃນລະບົບຄອມພິວເຕີ.

ຕົວຢ່າງ: ລະບົບເຊີເວີຂອງບໍລິສັດ ກໍ ໄດ້ຖືກໂຈມຕີຈາກແຮັກເກີ ເຮັດໃຫ້ລະບົບເຊີເວີ ບໍ່ສາມາດໃຊ້ງານເປັນປົກກະຕິ ແລະ ໄດ້ສ້າງຄວາມເສັຍຫາຍໃຫ້ກັບບໍລິສັດດັ່ງກ່າວ, ທາງບໍລິສັດ ກໍ ຄວນສະເໜີຂໍຄໍາປຶກສາ ແລະ ຄຳແນະນຳຈາກ ສູນສະກັດກັ້ນ ແລະ ແກ້ໄຂເຫດສຸກເສີນທາງຄອມພິວເຕີ, ກະຊວງໄປສະນີ, ໂທລະຄົມມະນາຄົມ ແລະ ການສື່ສານ ເພື່ອກວດສອບ, ຄົ້ນຫາແຫຼ່ງທີ່ມາຂອງການໂຈມຕີ ແລະ ປັບປຸງລະບົບໃຫ້ສາມາດກັບມາໃຊ້ງານໄດ້ເປັນປົກກະຕິ.

13. ມາດຕາ 22 ການແຈ້ງເຫດສຸກເສີນ ບຸກຄົນ, ນິຕິບຸກຄົນ ແລະ ການຈັດຕັ້ງ ທັງພາຍໃນ ແລະ ຕ່າງປະເທດ ທີ່ດຳລົງຊີວິດ, ເຄື່ອນໄຫວ ແລະ ນຳໃຊ້ລະບົບຄອມພິວເຕີ ແລະ ຫຼື ຂໍ້ມູນຄອມພິວເຕີຢູ່ໃນ ສປປ ລາວ ຕ້ອງແຈ້ງເຫດສຸກເສີນກ່ຽວກັບອາຊະຍາກຳທີ່ເກີດຂຶ້ນແກ່ລະບົບຄອມພິວເຕີຂອງຕົນຕໍ່ຂະແໜງໄປສະນີ, ໂທລະຄົມມະນາຄົມ ແລະ ການສື່ສານ ຕາມທີ່ໄດ້ກຳນົດໄວ້ໃນມາດຕາ 50 ແລະ 51 ຂອງກົດໝາຍວ່າດ້ວຍການຕ້ານ ແລະ ສະກັດກັ້ນອາຊະຍາກຳທາງລະບົບຄອມພິວເຕີ. ສຳລັບເຫດທົ່ວໄປ ເຊັ່ນ: ເວັບໄຊ, ເວັບເພຈ, ເວັບບອດ, ບັນດາຄຳຄິດເຫັນທາງສື່ສັງຄົມອອນລາຍທີ່ຕິດພັນກັບຂະແໜງການໃດ ແມ່ນ ໃຫ້ພົວພັນ, ປະສານງານ ແລະ ແຈ້ງຕໍ່ຂະແໜງການນັ້ນເປັນຜູ້ຄົນຄ້ວາ, ພິຈາລະນາໃຫ້ຂໍ້ມູນ ແລະ ຊື່ແຈງ.

ຕົວຢ່າງ: ລະບົບຄອມພິວເຕີຂອງບໍລິສັດ ກໍ ໄດ້ຕິດໄວຮັດ WannaCry Ransomware ຫຼື Wanna Decryptor 2.0 ຊຶ່ງສ້າງຄວາມເສັຍຫາຍໃຫ້ກັບບໍລິສັດດັ່ງກ່າວ ທາງບໍລິສັດ ກໍ ຄວນແຈ້ງເຫດສຸກເສີນ ຫາ ສູນສະກັດກັ້ນ ແລະ ແກ້ໄຂເຫດສຸກເສີນທາງຄອມພິວເຕີ, ກະຊວງໄປສະນີ, ໂທລະຄົມມະນາຄົມ ແລະ ການສື່ສານ ເພື່ອຂໍຄຳແນະນຳ, ວິທີການແກ້ໄຂ ແລະ ປ້ອງກັນບໍ່ໃຫ້ໄວຮັດດັ່ງກ່າວ ເກີດຂຶ້ນກັບລະບົບຄອມພິວເຕີອີກ. ການແຈ້ງເຫດສຸກເສີນສາມາດດຳເນີນດ້ວຍວິທີການ ດັ່ງນີ້:

1. ຄຳຮ້ອງຕາມແບບພິມ;
2. ໂທລະສັບ, ແຟັກ, ສາຍດ່ວນ;
3. ຈົດໝາຍເອເລັກໂຕຣນິກ;
4. ວິທີການອື່ນ.

14. ມາດຕາ 26 ການຝຶກອົບຮົມແມ່ນຂະແໜງການໄປສະນີ, ໂທລະຄົມມະນາຄົມ ແລະ ການສື່ສານ ປະສານສົມທົບກັບຂະແໜງການອື່ນ ແລະ ອົງການປົກຄອງທ້ອງຖິ່ນທີ່ກ່ຽວຂ້ອງ ຈັດຝຶກອົບຮົມໃຫ້ພະນັກງານ, ເຈົ້າໜ້າທີ່ກ່ຽວຂ້ອງ ກ່ຽວກັບວຽກງານຕ້ານ ແລະ ສະກັດກັ້ນອາຊະຍາກຳທາງລະບົບຄອມພິວເຕີ ລວມທັງວຽກງານການສືບສວນ-ສອບສວນ. ✓

ຕົວຢ່າງ: ສູນສະກັດກັ້ນ ແລະ ແກ້ໄຂເຫດການສຸກເສີນທາງຄອມພິວເຕີ ປະສານສົມທົບກັບເຈົ້າໜ້າທີ່ຕໍາຫຼວດສາກົນ ຈັດຝັກອົບຮົມວຽກງານການຕ້ານອາຊະຍາກໍາທາງລະບົບຄອມພິວເຕີ ໃນຫົວຂໍ້: ການກວດສອບຊ່ອງໂຫວ່ຂອງລະບົບຄອມພິວເຕີ, ການປ້ອງກັນລະບົບເຄືອຂ່າຍໃຫ້ມີຄວາມປອດໄພ ແລະ ການພິສູດຫຼັກຖານທາງເອເລັກໂຕຣນິກ ໂດຍເຊີນຕົວແທນ ຈາກບັນດາບໍລິສັດທີ່ໃຫ້ບໍລິການດ້ານໂທລະຄົມມະນາຄົມ, ທະນາຄານ, ວິຊາການຈາກກະຊວງປກຊ, ປກສ ແລະ ຂະແໜງການທີ່ກ່ຽວຂ້ອງ ເຂົ້າຮ່ວມ.

15. ມາດຕາ 28 ການສ້າງກົດຈະກຳປ້ອງກັນຂໍ້ມູນ ເພື່ອຮັບປະກັນຄວາມປອດໄພທາງລະບົບຄອມພິວເຕີ ແລະ ການປ້ອງກັນຂໍ້ມູນຄອມພິວເຕີ ຂະແໜງການໄປສະນີ, ໂທລະຄົມມະນາຄົມ ແລະ ການສື່ສານ, ຂະແໜງການປ້ອງກັນຄວາມສະຫງົບ, ຜູ້ໃຫ້ບໍລິການ ແລະ ຜູ້ຮັກສາຂໍ້ມູນ ຕ້ອງສ້າງກົດຈະກຳ ໃຫ້ຄວາມຮູ້ ດ້ານຄວາມປອດໄພ, ການນຳໃຊ້ລະບົບຄອມພິວເຕີ ເພື່ອໃຫ້ຮູ້ເຕັກນິກ ແລະ ວິທີປ້ອງກັນຂໍ້ມູນ ຢູ່ຕາມອົງການຈັດຕັ້ງຂອງລັດ, ເອກະຊົນ ແລະ ສະຖານການສຶກສາ.

ຕົວຢ່າງ: ສູນສະກັດກັ້ນ ແລະ ແກ້ໄຂເຫດສຸກເສີນທາງຄອມພິວເຕີ ໄດ້ສ້າງກົດຈະກຳກ່ຽວກັບວຽກງານຄວາມປອດໄພທາງໄຊເບີ ໂດຍການລົງໄປແຈກຢາຍແຜ່ນໂຄສະນາແຈ້ງເຕືອນໄພ ແລະ ແບບສອບຖາມ ຢູ່ບັນດາອົງການຈັດຕັ້ງຂອງລັດ, ເອກະຊົນ ແລະ ສະຖານບັນການສຶກສາ.

16. ມາດຕາ 30 ການເກັບກຳສະຖິຕິ ຂະແໜງການໄປສະນີ, ໂທລະຄົມມະນາຄົມ ແລະ ການສື່ສານ ແລະ ຂະແໜງການປ້ອງກັນຄວາມສະຫງົບ ຕ້ອງເກັບກຳສະຖິຕິ ກ່ຽວກັບອາຊະຍາກໍາທາງລະບົບຄອມພິວເຕີ ຕາມທີ່ໄດ້ລະບຸໄວ້ ໃນ ມາດຕາ 08 ຂອງກົດໝາຍວ່າດ້ວຍ ການຕ້ານ ແລະ ສະກັດກັ້ນອາຊະຍາກໍາທາງລະບົບຄອມພິວເຕີ ພ້ອມທັງສຶກສາຄົ້ນຄ້ວາເປັນແຕ່ລະໄລຍະ ເພື່ອຊອກຮູ້ເງື່ອນໄຂ ແລະ ສາເຫດທີ່ພາໃຫ້ເກີດອາຊະຍາກໍາທາງລະບົບຄອມພິວເຕີ.

17. ມາດຕາ 39 ຂໍ້ຫ້າມທົ່ວໄປ ແມ່ນການກຳນົດລະບຽບການ ເພື່ອຫ້າມ ບຸກຄົນ, ນິຕິບຸກຄົນ ແລະ ການຈັດຕັ້ງ ມີພຶດຕິກຳທີ່ເປັນການລະເມີດກົດໝາຍ ແລະ ລະບຽບການ, ຂໍ້ຫ້າມທົ່ວໄປ ມີ ດັ່ງນີ້:

17.1. ຫ້າລາຍ ຫຼື ສ້າງຄວາມເສັຍຫາຍໃຫ້ແກ່ອຸປະກອນເອເລັກໂຕຣນິກ, ຄອມພິວເຕີ ແລະ ສິ່ງອຳນວຍຄວາມສະດວກຕ່າງໆ ໃນການແລກປ່ຽນຂໍ້ມູນຂ່າວສານຜ່ານລະບົບຄອມພິວເຕີ ເປັນຕົ້ນໄປຮແກຣມອັນຕະລາຍ, ໄວຣັດ, ການໂຈມຕີລະບົບຄອມພິວເຕີ ແລະ ອື່ນໆ;

17.2. ສົມຮູ້ຮ່ວມຄິດກັບບຸກຄົນໃດໜຶ່ງ ເພື່ອເຜີຍແຜ່ສິ່ງລາມົກ ເປັນຕົ້ນ ຮູບ, ພາບເຄື່ອນໄຫວ, ສຽງ ແລະ ວິດີໂອ ກ່ຽວກັບອະໄວຍະວະເພດ ແລະ ພຶດຕິກຳທາງເພດຂອງຄົນ ໂດຍຜ່ານສື່ສັງຄົມອອນລາຍ;

17.3. ທວງເອົາ, ຂໍເອົາ, ໃຫ້ ແລະ ຮັບສິນບິນ ເພື່ອໃຫ້ໄດ້ມາດຕະການປ້ອງກັນສະເພາະຂອງລະບົບຄອມພິວເຕີ ໄປເປີດເຜີຍ ແລະ ສ້າງຄວາມເສັຍຫາຍໃຫ້ແກ່ລັດ, ບຸກຄົນ, ນິຕິບຸກຄົນ, ການຈັດຕັ້ງ ແລະ ສັງຄົມ.

18. ມາດຕາ 40 ຂໍ້ຫ້າມສຳລັບຜູ້ໃຫ້ບໍລິການ ແມ່ນການກຳນົດລະບຽບການ ເພື່ອຫ້າມ ຜູ້ໃຫ້ບໍລິການມີພຶດຕິກຳທີ່ເປັນການລະເມີດກົດໝາຍ ແລະ ລະບຽບການ, ຂໍ້ຫ້າມສຳລັບຜູ້ໃຫ້ບໍລິການ ໄດ້ກຳນົດໄວ້ ດັ່ງນີ້:

18.1. ລົບຂໍ້ມູນທີ່ຈາລະຈອນທາງລະບົບຄອມພິວເຕີ ເຊັ່ນ: ຂໍ້ມູນຫຼັກຖານການໂທລະສັບ, ຂໍ້ມູນການສົ່ງຂໍ້ຄວາມສັ້ນ, ຂໍ້ມູນການນຳໃຊ້ອິນເຕີເນັດ ແລະ ອື່ນໆ ກ່ອນເກົ້າສິບວັນ ໃນກໍລະນີເຊື່ອມຕໍ່ ແລະ ກ່ອນສາມຮ້ອຍຫົກສິບຫ້າວັນ ໃນກໍລະນີບໍ່ເຊື່ອມຕໍ່; ✓

18.2. ລົບຂໍ້ມູນຜູ້ຊົມໃຊ້ລະບົບຄອມພິວເຕີທີ່ສ້າງຄວາມເສັຍຫາຍ ກ່ອນເກົ້າສິບວັນ ເຊັ່ນ: ຂໍ້ມູນຫຼັກຖານການໂທລະສັບ, ຂໍ້ມູນການສົ່ງຂໍ້ຄວາມສັ່ນ, ຂໍ້ມູນການນຳໃຊ້ອິນເຕີເນັດ ແລະ ອື່ນໆ ເພື່ອເກັບຮັກສາ ແລະ ສະໜອງຂໍ້ມູນດັ່ງກ່າວ ໃຫ້ເຈົ້າໜ້າທີ່ ມີສິດອຳນາດກ່ຽວຂ້ອງ;

18.3. ສະໜອງຂໍ້ມູນທີ່ບໍ່ຖືກຕ້ອງ ໃຫ້ເຈົ້າໜ້າທີ່ ແລະ ພະນັກງານທີ່ກ່ຽວຂ້ອງ ເປັນຕົ້ນ: ຂໍ້ມູນຄອມພິວເຕີ ຫຼື ອຸປະກອນເອເລັກໂຕຣນິກທີ່ນຳໃຊ້ກະທຳຄວາມຜິດ, ຂໍ້ມູນຄວາມລັບຂອງອົງການຈັດຕັ້ງ, ຂໍ້ມູນດ້ານຄວາມໝັ້ນຄົງຂອງຊາດ, ຂໍ້ມູນທາງດ້ານການຄ້າ, ຂໍ້ມູນທຸລະກຳທາງການເງິນ, ຂໍ້ມູນທີ່ລັກສະນະທຳລາຍການປະຕິບັດງານຂອງລະບົບຄອມພິວເຕີ, ຂໍ້ມູນທີ່ເປັນສິ່ງລາມີກອນາຈານ, ຂໍ້ມູນການຕັດຕໍ່ເນື້ອໃນ, ຮູບ, ພາບເຄື່ອນໄຫວ, ສຽງ ແລະ ວິດີໂອ, ຂໍ້ມູນອື່ນທີ່ກ່ຽວຂ້ອງ.

18.4. ເປີດເຜີຍຂໍ້ມູນຂອງຜູ້ໃຊ້ບໍລິການ ໂດຍບໍ່ໄດ້ຮັບອະນຸຍາດ ເຊັ່ນ: ຂໍ້ມູນປະຫວັດການໂທລະສັບ, ຂໍ້ມູນການສົ່ງຂໍ້ຄວາມສັ່ນ, ຂໍ້ມູນການນຳໃຊ້ອິນເຕີເນັດ ແລະ ອື່ນໆ;

18.5. ສ້າງເງື່ອນໄຂ ຫຼື ອຳນວຍຄວາມສະດວກໃຫ້ແກ່ການເຄື່ອນໄຫວກ່ອນອາກຳທາງລະບົບຄອມພິວເຕີ ເປັນຕົ້ນ ການສົມຮູ້ຮ່ວມຄິດ, ໃຫ້ຂໍ້ມູນທີ່ເປັນຄວາມລັບ, ສະໜອງອຸປະກອນ ແລະ ອື່ນໆ.

19. ມາດຕາ 41 ຂໍ້ຫ້າມສຳລັບເຈົ້າໜ້າທີ່ ແລະ ພະນັກງານທີ່ກ່ຽວຂ້ອງ ແມ່ນ ການກຳນົດລະບຽບການ ເພື່ອຫ້າມມີພຶດຕິກຳທີ່ເປັນການລະເມີດກົດໝາຍ ແລະ ລະບຽບການ, ຂໍ້ຫ້າມສຳລັບເຈົ້າໜ້າທີ່ ແລະ ພະນັກງານທີ່ກ່ຽວຂ້ອງ ໄດ້ກຳນົດໄວ້ ດັ່ງນີ້:

19.1. ເປີດເຜີຍຄວາມລັບຂອງ ລັດ, ທາງລັດຖະການ, ຂອງ ບຸກຄົນ, ນິຕິບຸກຄົນ ຫຼື ການຈັດຕັ້ງ ຜ່ານລະບົບຄອມພິວເຕີ ເຊັ່ນ: ຂໍ້ມູນຄວາມລັບຂອງອົງການຈັດຕັ້ງ, ຂໍ້ມູນດ້ານຄວາມໝັ້ນຄົງຂອງຊາດ, ຂໍ້ມູນທາງດ້ານການຄ້າ, ຂໍ້ມູນທຸລະກຳທາງການເງິນ ແລະ ອື່ນໆ;

19.2. ເປີດເຜີຍລະຫັດເຂົ້າເຖິງລະບົບຄອມພິວເຕີ ແລະ ມາດຕະການປ້ອງກັນສະເພາະຂອງຂະແໜງການຕົນ ເປັນຕົ້ນ: ວິທີການ, ຂໍ້ກຳນົດ ແລະ ລະບຽບການສະເພາະໃນການຮັກສາຄວາມປອດໄພຂອງລະບົບຄອມພິວເຕີ.

19.3. ສົ່ງມອບ ຂໍ້ມູນຄອມພິວເຕີ, ຂໍ້ມູນຈາລະຈອນ ຜ່ານລະບົບຄອມພິວເຕີ ຫຼື ຂໍ້ມູນຂອງຜູ້ໃຊ້ບໍລິການໃຫ້ແກ່ບຸກຄົນອື່ນ ຍົກເວັ້ນການສົ່ງມອບ ເພື່ອປະໂຫຍດໃນການນຳເນີນຄະດີ ເຊັ່ນ: ການປະຕິບັດຄຳສັ່ງ ຫຼື ກຳລະນີໄດ້ຮັບອະນຸຍາດ ຈາກອົງການດຳເນີນຄະດີ;

19.4. ກົດໝວງ, ຖ່ວງດຶງ ແລະ ປອມເອກະສານ ກ່ຽວກັບຂໍ້ມູນທີ່ເປັນການກະທຳຜິດທາງລະບົບຄອມພິວເຕີ. ໃນກໍລະນີ ມີຂໍ້ມູນທີ່ເປັນການກະທຳຜິດທາງລະບົບຄອມພິວເຕີ ເມື່ອມີຄວາມຕ້ອງການນຳໃຊ້ຂໍ້ມູນດັ່ງກ່າວ, ເຈົ້າໜ້າທີ່ ແລະ ພະນັກງານທີ່ກ່ຽວຂ້ອງ ຕ້ອງອຳນວຍຄວາມສະດວກໃຫ້ຄວາມຮ່ວມມື, ສະໜອງຂໍ້ມູນໃຫ້ຄົບຖ້ວນ ແລະ ຖືກຕ້ອງຕາມຂໍ້ມູນຄວາມຈິງ.

20. ມາດຕາ 44 ການແຈ້ງຄວາມ, ການລາຍງານ ຫຼື ການຮ້ອງຟ້ອງ ກ່ຽວກັບການກະທຳຜິດທາງລະບົບຄອມພິວເຕີ ບຸກຄົນ, ນິຕິບຸກຄົນ ຫຼື ການຈັດຕັ້ງ ສາມາດແຈ້ງ ຫຼື ຍື່ນຕໍ່ ອົງການສືບສວນ-ສອບສວນຂອງເຈົ້າໜ້າທີ່ຕໍາຫຼວດ ຫຼື ອົງການໄອຍະການປະຊາຊົນ ເປັນຕົ້ນ ການກະທຳຜິດທາງລະບົບຄອມພິວເຕີ ຫຼື ພຶດຕິກຳທີ່ເປັນອາຊະຍາກຳທາງລະບົບຄອມພິວເຕີ ທີ່ລະບຸໄວ້ໃນມາດຕາ 8 ຂອງກົດໝາຍວ່າດ້ວຍການຕ້ານ ແລະ ສະກັດກັ້ນອາຊະຍາກຳທາງລະບົບຄອມພິວເຕີ. ✓

ອົງການສືບສວນ-ສອບສວນຂອງເຈົ້າໜ້າທີ່ຕໍາຫຼວດ ຫຼື ອົງການໄອຍະການປະຊາຊົນ ຕ້ອງພິຈາລະນາການແຈ້ງຄວາມ, ການລາຍງານ ຫຼື ການຮ້ອງຟ້ອງ ບໍ່ໃຫ້ເກີນ ຫ້າວັນ ລັດຖະການ ນັບແຕ່ວັນໄດ້ຮັບການແຈ້ງຄວາມ, ການລາຍງານ ຫຼື ການຮ້ອງຟ້ອງ ເປັນຕົ້ນໄປ ໃນກໍລະນີມີຄວາມຫຍຸ້ງຍາກສັບສົນ ການພິຈາລະນາດັ່ງກ່າວ ແມ່ນ ບໍ່ໃຫ້ເກີນ ສິບວັນ ລັດຖະການ.

ຕົວຢ່າງ: ທ້າວ ກໍ ໄດ້ຕັດຕໍ່ ຮູບພາບຂອງ ນາງ ຂໍ ນໍາໄປເຜີຍແຜ່ທາງເຟສບຸກ (Facebook) ໂດຍບໍ່ໄດ້ຮັບອະນຸຍາດ ຊຶ່ງສ້າງຄວາມເສັຍຫາຍໃຫ້ແກ່ຜູ້ກ່ຽວ ຖ້າຫາກວ່າ ນາງ ຂໍ ຕ້ອງການຮຽກຮ້ອງຂໍຄວາມເປັນທໍາ ນາງ ຂໍ ຕ້ອງນໍາເອົາຂໍ້ມູນ, ຫຼັກຖານ ແຈ້ງຄວາມຕໍ່ ອົງການສືບສວນ-ສອບສວນຂອງເຈົ້າໜ້າທີ່ຕໍາຫຼວດ ເພື່ອພິຈາລະນາ ຕາມຫຼັກການສືບສວນ-ສອບສວນຄະດີທາງລະບົບຄອມພິວເຕີ.

III. ການຈັດຕັ້ງປະຕິບັດ

ມອບໃຫ້ ສຸນສະກັດກັ້ນ ແລະ ແກ້ໄຂເຫດສຸກເສີນທາງຄອມພິວເຕີ ປະສານສົມທົບກັບພາກສ່ວນທີ່ກ່ຽວຂ້ອງ ແລະ ອົງການປົກຄອງທ້ອງຖິ່ນ ຈັດຕັ້ງໂຄສະນາ, ເຜີຍແຜ່, ແນະນໍາ ແລະ ປະຕິບັດຄໍາແນະນໍາສະບັບນີ້ໃຫ້ໄດ້ຮັບຜົນດີ.

ບັນດາກະຊວງ, ອົງການທຽບເທົ່າກະຊວງ ແລະ ອົງການປົກຄອງທ້ອງຖິ່ນ, ບຸກຄົນ, ນິຕິບຸກຄົນ ພາຍໃນ ສປປລາວ ຈົ່ງຮັບຮູ້ ແລະ ນໍາໄປຈັດຕັ້ງປະຕິບັດໃຫ້ຖືກຕ້ອງ.

IV. ຜົນສັກສິດ

ຄໍາແນະນໍາສະບັບນີ້ ມີຜົນສັກສິດແຕ່ວັນລົງລາຍເຊັນ ແລະ ພາຍຫຼັງທີ່ໄດ້ລົງໃນຈົດໝາຍເຫດທາງລັດຖະການສືບຫ້າວັນ.

ລັດຖະມົນຕີ


ປອ. ທັນສະໄໝ ກິມມະສິດ