ISSUE NO 03

OCTOBER 2023

Cyber Guardian

A Publication on Online Safety

SECURITY சைபர் பாதுகாப்புக்கான 10 படி முறைகள்

1. இடையூறு, இன்னல்களை தடுப்பதற்கான செயல்முறையிலான நிருவாக முறை
உங்கள் நிறுவனத்தில் சிரேஷ்ட முகாமையாளர்கள் மற்றும் பணிப்பாளர்கள் குழுவுடன் இணைந்து இடையூறு இன்னல்களை தடுப்பதற்கான செயல்முறையிலான நிருவாக முறையை நிறுவுவது அவசியம். இடையூறு இன்னல்களை தடுக்கும் முகாமைத்துவ செயல் முறையின் அடிப்படையில், உங்கள் தகவல் மற்றும் தகவல் தொழில்நுட்ப அமைப்புக்கான பாதிப்புக்களை மதிப்பிட்டு பாதுகாப்பதற்கான முகாமைத்துவம் இடம்பெறும்.

2. தீங்குநிர (ஆயடறயசந) லை தடுத்தல்
தீம்பொருளால் (ஆயடறயசந) உங்கள் நிறுவனத்திற்கு பாதிப்பு ஏற்படுவதைத் தடுக்க, சரியான எதிர்ப்பு மென்பொருளை நிறுவி செயல்படுத்துவது அவசியம்.

3. பாதுகாப்பான அமைவடிவாக்கம்
எப்போதும் உங்கள் கணினி மென்பொருள் தகவல் அமைப்பு மற்றும் உபகரணங்களை சமீபத்திய இணைப்புடன் ீயவஉா புதுப்பித்துக்கொள்ள வேண்டும்.

4. வெளிப்புற இணைப்புக் கருவிகளைப் பயன்படுத்துவதைக் கட்டுப்படுத்துதல்
கணினிகளுக்கான வெளிப்புற இணைப்புக் கருவிகளை (உதாரணமாக: ருளுடீ ளவஉைமள, நுஒவநசயெட ர்யசன னுளைம) பயன்படுத்துவதை எப்போதும் கட்டுப்படுத்துங்கள். அவற்றை இணைத்து இயக்கும் முன், தீம்பொருள் எதிர்ப்பு மென்பொருளைக் கொண்டு ளுஉயடீ ஸ்கேன் செய்வதை உறுதிசெய்து கொள்ளுவதற்கான வழி முறையை உறுதிப்படுத்திக்கொள்ளுங்கள்.

5. பயன்படுத்துபவருக்கான கல்வி மற்றும் விழிப்புணர்வ
பெரும்பாலான சைபர் பாதுகாப்பு குறித்த அச்சுறுத்தல்கள் அறியாமையால் ஏற்படுகின்றன. இதனால் உபயோகிப்பவர்களுக்கு தகவல், கல்வி ஆகிய விடயங்களில் போதிய அறிவும் மற்றும் பயிற்சியும் அளிக்க வேண்டியது அவசியம்.

6. அணுகல் நிர்வாக அமைப்பு
நிறுவனத்தில் உள்ள கணினிகள் மற்றும் கட்டமைப்புகளுக்கான அணுகலைக் கட்டுப்படுத்த அடையாள முகாமைத்துவ செயல்முறை பராமரிக்கப்படுவதுடன், இதன் ஊடாக தரவு மற்றும் அமைப்புகளுக்கான அங்கீகாரமற்ற அணுகலை தவிர்க்கலாம். மேலும் எப்போதும் எண்கள் மற்றும் சிறப்பு குறியீடுகளைக் (டுழறநசஉயளந டநவவநசள, ளுிநஉயைட ஊாயசயஉவநசள, ரேஅடிநசள) கொண்ட கடவுச்சொற்களைப் பயன்படுத்தவும் , குறைந்தது 8 எழுத்துகள் அல்லது அதற்கு மேற்பட்டவற்றைப் பயன்படுத்த வேண்டும்.

7. காப்பு மூலோபாயம்
நிறுவனத்தில் உள்ள தரவு மற்றும் செயற்பாட்டு டீயஉமரி பதிவுகளை தொடர்ச்சியாக பிரதான அமைப்பிலிருந்து தனித்தனியாக சேமிப்பதுடன் அவற்றை பிரதான கட்டமைப்பில் தனித்தனியாக பாதுகாக்க வேண்டும்.

8. நிகழ்வுகளை முகாமைத்தும் செய்வதற்கான திட்டம்
ஒரு சம்பவத்திற்கு பதிலளிப்பதற்காக அமைப்புக்கு பொருத்தமான சம்பவ முகாமைத்துவ திட்டம் வகுக்கப்படுவதுடன், அதன் செயல்திறன் தொடர்ந்து மதிப்பீடு செய்யப்பட வேண்டும்.

9. வீட்டில் இருந்தவாறே கடமைகளில் ஈடுபடுதல்
வீட்டில் இருந்தவாறே இணையத்தளம் மூலம் கடமைகளை செய்வதற்கான கொள்கையை உருவாக்கி, அதற்கேற்ப செயல்பட ஊழியர்களுக்கு பயிற்சி அளிக்கவும். இவ்வாறு தொலைதூரத்தில் வேலை செய்யும் போது தரவு மற்றும் சாதனங்களைப் பாதுகாக்க அடிப்படை பாதுகாப்பு முறைகளை அறிமுகப்படுத்த வேண்டும்.

10. பாதுகாப்பு மதிப்பீடுகள்
நிறுவனத்தினால் அதன் கணினி கட்டமைப்புகள் மற்றும் தரவைப் பாதுகாக்க, பாதுகாப்பு தணிக்கையை மேற்கொள்வதுடன் அதன் மூலம் அடையாளம் காணப்பட்ட பாதுகாப்பு குறைபாடுகள் சரி செய்யப்பட வேண்டும்.இந்த தணிக்கைகளை கணினி கட்டமைப்பில் செயல்படுத்துவதற்கு முன் அல்லது தற்போது இயங்கும் கணினி அமைப்பில் மாற்றத்தை ஏற்படுத்திய பின் அல்லது கணினி அமைப்பு நிறுவப்பட்டுள்ள ஊடகத்தில் (மொழியில்) மாற்றம் செய்த பிறகு அல்லது இணைய தாக்குதலுக்குப் பிறகு செய்யப்பட வேண்டும்.

News

இலங்கை சர்ட் நிறுவனம் (ளுசஅ டுயமெய ஊநுசுவு ளுசஅ டுயமெய ஊநுசுவு) தகவல் பாதுகாப்பு அதிகாரிகள் (ஐளுழு), உதவி தகவல் பாதுகாப்பு அதிகாரிகள் (யுஐளுழு) மற்றும் ஏனைய அரசாங்க அதிகாரிகளுக்கு இணைய பாதுகாப்பு (அடிப்படைகள் மற்றும் கோட்பாட்டு விடயங்கள்) தொடர்பான செயல் அமர்வுகளை நடத்தி வருகிறது. இந்த அமர்வுகளின் முக்கிய நோக்கம், இணைய பாதுகாப்பு உத்திகள், பயன்பாடு குறித்து இவர்களுக்கு தெளிவுபடுத்துவதாகும்

இலங்கை கணினி அவசர தயார்நிலையம் (CERT) புதிதாக நியமிக்கப்பட்ட ICT ஆசிரியர்களுக்கான பயிற்சி செயல் அமர்வை நடத்தியது.

கல்வி அமைச்சினால் ஏற்பாடு செய்யப்பட்ட இந்நிகழ்வில் அனைத்து மாகாணங்களையும் பிரதிநிதித்துவப்படுத்தி சுமார் 130 ICT ஆசிரியர்கள் கலந்துகொண்டனர். இரண்டாம் கட்டப் பயிலரங்கில் சுமார் 100 ஆசிரியர்கள் கலந்துகொண்டனர்.

இலங்கை சர்ட் நிறுவனத்தின் பொறுப்பு

இலங்கை கணினி அவசர தயார்நிலை (CERT) அல்லது National Center for Cyber Security என்பது சைபர் பாதுகாப்பிற்கான தேசிய நிலையமாகும். இது நாட்டின் இணையவெளியை இணைய அச்சுறுத்தல்களிலிருந்து பாதுகாக்கும் தேசிய பொறுப்பைக் கொண்டுள்ளது. தற்போது தொழில்நுட்ப அமைச்சின் கீழ் செயல்பட்டுவருகிறது. அத்தோடு இது 2006 ஆம் ஆண்டு அரசாங்கத்திற்கு சொந்தமான ஒரு தனியார் நிறுவனமாக அமைக்கப்பட்டது.

இலங்கையின் CERT நிறுவனம் இன்று வலையமைக்கப்பட்ட உலகளாவிய இணைய சம்பவங்களுக்கு பதில் அளிக்கக்கூடிய நிலையமாக மேம்பட்டுள்ளது. நன்கு பயிற்றுவிக்கப்பட்ட மற்றும் தகுதிவாய்ந்த இணைய பாதுகாப்பு வல்லுநர் பணியாளர்களை இது கொண்டுள்ளது. இலங்கை CERT நிறுவனம் Global CERT networks வலையமைப்புகளின் பங்குதாரராகவும் செயல்பட்டுவருகிறது. சர்வதேச FIRST (The International FIRST (Incident Response Forum), ஐரோப்பிய ஒன்றியம் மற்றும் உலக வங்கி ஆகியவற்றின் Asia Pacific CERT, Cyber4Dev European Union ஆசிய பசிபிக் CERT, ஊலடிநச4னுநள உறுப்பினராக இணைந்து நாட்டிற்கு சிறந்த இணைய பாதுகாப்பு சூழலை உருவாக்கும் பணியை முன்னெடுத்துவருகிறது.

இலங்கையில் இணையத் தாக்குதல்களின் தாக்கத்தைத் தடுப்பதற்கு அல்லது தணிப்பதில் உலகளாவிய அரசாங்க நிறுவனங்களுக்கு உதவ இலங்கை செர்ட் நிறுவனம் செயல்படுகிறது. இதற்கு மேலாக தேசிய இணையப் பாதுகாப்புக் கொள்கை மற்றும் நடைமுறைகளும் அறிமுகப்படுத்தப்பட்டுள்ளன. குறிப்பாக இணையத் தாக்குதல்களில் இருந்து அரசு நிறுவனங்களைத் பாதுகாத்துக் கொள்ள அவற்றை தயார்படுத்துதல் மற்றும் தாக்குதல் நடந்தால், அவற்றுக்கு பதிலடியை வழங்குவது CERT நிறுவனத்தின் முதன்மைப் பொறுப்பாக அறிமுகப்படுத்தலாம். இதேபோன்று, இணையப் பாதுகாப்பில் அரசத்துறையில் வலுவான பணியாளர்களை உருவாக்குதல், பல்வேறு சமூகப் பிரிவுகளுக்கு தெளிவுபடுத்தல் மற்றும் இணைய அச்சுறுத்தல்களை எதிர்கொள்ளும் நிறுவனங்கள் மற்றும் தனிநபர்கள் தங்கள் பிரச்சினைகளைத் தீர்க்க உதவுதல் இதன் பயன்களாக அமைந்துள்ளன.

Circular

அரசாங்கத்தின் உத்தியாகபூர்வ அலுவல்களுக்கு gov.lk

அனைத்து அரசாங்க நிறுவங்களும் தங்களது உத்தியாகபூர்வ தகவல் தொடர்புகளுக்கு அதிகாரப்பூர்வ மின்னஞ்சல் முகவரிகளை பயன்படுத்த வேண்டும். இந்த உத்திபோகபூர்வ மின்னஞ்சல் (E-Mail) தனிப்பட்டவிட ங்களுக்காக பயன்படுத்தக் கூடாது. அத்தோடு, அரசாங்க நிறுவனங்களுக்கான பாதுகாப்பு மற்றும் இனணப் பாதுகாப்புக் கொள்கையின் கீழ் இந்த விடயம் அறிவிக்கப்பட்டுள்ளது. ஜாதிபதியின் செயலாளர் வெளியிட் SP/SB/10/13 சுற்றறிக்கையின் ஊடாக இது உறுதிப்படுத்தப்பட்டுள்ளது. உத்தியோகபூர்வ மின்னஞ்சல் என்பது அரசாங்கத்தால் வழங்கப்படும் gov.lk மின்னஞ்சல் ஆகும்.

Gmail (அஞ்சல் முறையை) லை பயன்படுத்துபவர்களைப் பாதுகாப்பதற்கான புதிய வழிகாட்டுதல்கள்

மின்னஞ்சல் தரவு திருட்டு மற்றும் தீங்கிழைக்கும் தீம்பொருள் மென்பொருள் விநியோகத்திலிருந்து மின்னஞ்சலைப் பாதுகாப்பதற்கும் வலுப்படுத்துவதற்குமாக மின்னஞ்சல்களை அனுப்புபவர்களின் நலன் கருதி புதிய வழிகாட்டுதல்களை எதிர்வரும் பெப்ரவரி மாதம் அறிமுகப்படுத்த கூகுள் புழுடந நிறுவனம் தயாராகி வருகிறது.

மின்னஞ்சல் மோசடி மற்றும் தரவு திருட்டுக்கு எதிரான பாதுகாப்பை வலுப்படுத்த மின்னஞ்சல் பயன்படுத்துவோரின் கணக்குகளுக்கு SPF/DKIM and DMARC அங்கீகாரம் அறிமுகப்படுத்தப்படும். இது தரவுகள் திருடப்படுவதை தடுக்க உதவுவதுடன், கடத்தல் மற்றும் தீங்கிழைக்கும் மென்பொருளின் சுற்றோட்டத்தை தடுக்கவும் பயன்படுகிறது. நச்சரிப்பான வணிக மின்னஞ்சல்களைத் தவிர்க்கவும் Icons - சின்னங்களில் இருந்து பதிவு நீக்கலையும் மேற்கொள்ள முடியும். அத்தோடு அந்த வணிக நிறுவன வியாபாரங்ளுடன், இரண்டு நாட்களுக்குள் தொடர்பை தடுக்க நடவடிக்கை எடுக்க வேண்டும். இப்போதும் கூட, ஜிமெயி (Gmail) லின் செயற்கை நுண்ணறிவு அடிப்படையிலான பாதுகாப்பு 99.9% க்கும் அதிகமான தரவு திருட்டு மற்றும் தீம்பொருள் மூலமான மின்னஞ்சல் தொடர்புகளையும் தடுக்கப்படுவதாக கூகுள் நிறுவனம் தெரிவித்துள்ளது. அதன்படி, ஒரு நாளைக்கு கிட்டத்தட்ட 15 பில்லியன் தேவையற்ற மின்னஞ்சல்களை வெற்றிகரமாகத் தடுக்க முடிகிறது.

Laws & policies

தகவல், தகவல் தொழில்நுட்பம் மற்றும் இணையப் பாதுகாப்பு தொடர்பான கட்டளை சட்டங்கள்

- 2007 ஆம் ஆண்டின் 24 ஆம் இலக்க. கணினி வழிக்குற்றச் சட்டம்
- 2006 ஆம் ஆண்டின் 30 ஆம் இலக்க கொடுப்பனவு உபாயங்களின் மோசடிகள் சட்டம்
- 2022 ஆம் ஆண்டின் 9 ஆம் இலக்க, தனிப்பட்ட தரவுப் பாதுகாப்புச் சட்டம்
- 2006 ஆம் ஆண்டின் 19 ஆம் இலக்க இலத்தரனியல் கொடுக்கல் வாங்கல் சட்டம்
- அரசு நிறுவனங்களுக்கான தகவல் மற்றும் சைபர் பாதுகாப்புக் கொள்கை 2023.