ISSUE NO 01

AUGUST 2023

Cyber Guardian

Publication for your online safety

SRI LANKA CERT|CC
Sri Lanka Computer Emergency Readiness Team
Coordination Centre

Policies

அரசாங்க நிறுவனங்களுக்கான வலுவான தகவல் மற்றும் சைபர் பாதுகாப்புக் கொள்கையை முன்னெடுப்பதில் இலங்கை (CERT) மற்றும் தொழில்நுட்ப அமைச்சு ஆகியன கூட்டு சக்திகள்

டிஜிட்டல் பாதுகாப்பை மேம்படுத்துவதற்கும், முக்கியமான தகவல்களைப் பாதுகாப்பதற்கும் முன்னோக்கிச் செயல்படும் நடவடிக்கையின் கீழ் இலங்கை கணினி அவசர தயார்நிலை அணி (CERT) அரசாங்க நிறுவனங்களுக்கான விரிவான தகவல் மற்றும் இணைய பாதுகாப்பு கொள்கையை முன்வைத்துள்ளது. அரசாங்க நிறுவனங்களுக்கான தகவல் மற்றும் இணையப் பாதுகாப்புக் கொள்கைக்கு 2022 ஆண்டு ஆகஸ்ட் மாதம் அமைச்சரவையின் அங்கீகாரம் கிடைத்தது. அத்துடன் இந்த ஆண்டு முதல் அதனை நடைமுறைப்படுத்துவதற்கு அமைச்சு துரித நடவடிக்கைகளை மேற்கொண்டுள்ளது. இலங்கை செர்ட் (CERT) என்பது நாட்டில் இணைய பாதுகாப்பு அச்சுறுத்தல் சம்பவங்களுக்கு உடனடி பதிலளிக்கும் தயார் நிலை நிறுவனமாவதுடன் , இணைய (சைபர் பாதுகாப்பு) பாதுகாப்புக் கொள்கையை வகுத்தல் மற்றும் அதனுடன் தொடர்புபட்ட சேவைகளை வழங்கும் அரசாங்க நிறுவனமாகும். இந்த இணைய பாதுகாப்பு கொள்கை அனைத்து அரசு நிறுவனங்களுக்கும் ஏற்புடையது.

முக்கிய நோக்கம்

இணைய அச்சுறுத்தலை எதிர்கொள்வதற்கான (சைபர்) தயார்நிலை:
இலங்கை (CERT), தொழில்நுட்ப அமைச்சின் ஒத்துழைப்புடன் இணைய அச்சுறுத்தல்களுக்கு எதிராக அரசாங்க நிறுவனங்களைத் தயார்படுத்துவதற்கான திட்டத்தைச் செயல்படுத்துவதுடன், இதில் இணைய அச்சுறுத்தல் பகுப்பாய்வு, இடர் மதிப்பீடுகள் மற்றும் செயலூக்கமான பாதுகாப்பு நடவடிக்கைகள் ஆகியவையும் அடங்கியுள்ளன.

கொள்கை கட்டமைப்பு:
அரசாங்க நிறுவனங்கள் ஊடான முழு தகவல்கள் தொடர்பிலான பாதுகாப்பிற்கான தெளிவான வழிகாட்டுதல்கள், தரநிலைகள் மற்றும் சிறந்த நடைமுறைகளை நிறுவ வலுவான மேம்படுத்தப்பட்ட கொள்கை கட்டமைப்பு உருவாக்கப்பட்டுள்ளது. இந்தக் கொள்கை கட்டமைப்பு தரவு பாதுகாப்பு, சம்பவங்களுக்கான பதில் அளிக்கும் நடைமுறைகளை உள்ளடக்கியுள்ளன.

திறன் மேம்பாடு:
இணைய அச்சுறுத்தல்களை திறம்பட கண்டறிந்து தணிக்க தேவையான திறன்களை அரசு ஊழியர்களுக்கு வழங்குவதற்கான பயிற்சி மற்றும் திறன்களை மேம்படுத்துவதற்கான திட்டங்களும் முன்னெடுக்கப்படும். இந்த நடவடிக்கை சைபர் பாதுகாப்பு விழிப்புணர்வு கலாச்சாரத்தை உருவாக்கும் என்பதே எதிர்பார்ப்பாகும்.

அரச - தனியார் துறை ஒத்துழைப்பு:
தனியார் துறை மற்றும் சர்வதேச இணைய பாதுகாப்பு நிறுவனங்களுடனான ஒத்துழைப்பு, இலங்கையில் இணைய பாதுகாப்பு செயல்முறையை வலுப்படுத்த பயன்படுத்தப்படும். இது அறிவுப் பகிர்வு மற்றும் இணைய அச்சுறுத்தல்கள் பற்றிய விழிப்புணர்வை ஊக்குவிக்க வழிவகுக்கும்.

அரசாங்க நிறுவனங்களை வலுப்படுத்தல்:
இந்தக் கொள்கையை நடைமுறைப்படுத்துவது அரசாங்கத்தின் தரவு, சேவைகள் மற்றும் பிரஜைகளின் தகவல்களைப் பாதுகாப்பதில் இன்றியமையாத முதல் படி நடவடிக்கையாகும். இது இலங்கையின் டிஜிட்டல் அபிவிருத்திச் செயல்முறையை வலுப்படுத்துவதுடன், இணையச் சம்பவங்களை தடுப்பதற்கான ஒருங்கிணைக்கப்பட்ட செயலூக்கமான வேலைத்திட்டமாகும்.

பிரஜைகளுடன் தொடர்பை ஏற்படுத்தல்:
இணைய பாதுகாப்பு தொடர்பிலான செயல்பாட்டில் பிரஜைகள் நிறை வேற்றுவதற்கான பொறுப்புக்களை இலங்கை CERT நிறுவனம் குடிமக்களை ஊக்குவிக்கும். தேசிய இணையப் பாதுகாப்பைப் பேணுவதற்கு, சந்தேகத்திற்கிடமான இணையத்தள செயல்பாட்டு தகவல்களை முறையிடுதல் மற்றும் பாதுகாப்பான டிஜிட்டல் பழக்கவழக்கங்களை பயிற்றுவித்தல் முதலானவற்றை பின்பற்றுவது அவசியமாகும். இலங்கை CERT நிறுவனம் மற்றும் தொழில்நுட்ப அமைச்சுக்கு இடையிலான கூட்டு முயற்சியானது இணைய பாதுகாப்புக்கான அரசாங்கத்தின் அர்ப்பணிப்பை கோடிட்டுக் காட்டுகிறது. இந்தக் கொள்கையை நடைமுறைப்படுத்துவதன் மூலமும் இணைய விழிப்புணர்வின் கலாச்சாரத்தை வளர்ப்பதன் மூலமும், இலங்கை பாதுகாப்பான டிஜிட்டல் நாடு என்பது உறுதி செய்யப்படும்.

Security

கணினி பாதுகாப்பிற்கான ஒரு டிஜிட்டல் கண்காணிப்பு பொறி முறை

வேகமாக வளர்ந்து வரும் தொழில்நுட்ப முன்னேற்றத்தில் உங்கள் டிஜிட்டல் தொழில் நுட்பத்தின் இருப்பை பாதுகாக்க கணினி வைரஸ் என்ற “காவலர்” இன்றியமையாதது. இத் திட்டம் பெரும்பாலும் வைரஸ் தடுப்பு மென்பொருள் அல்லது பாதுகாப்பு தொகுப்புகள் என குறிப்பிடப்படும், இந்த நிரல்கள் கணினி வைரஸ்கள், மால்வேர் மற்றும் சைபர் (Malware and Cyber threats) அச்சுறுத்தல்கள் ஏற்படுவதற்கு முன்பு அவைகளுக்கு எதிராக முன்னோடி காவலர்களை போன்று செயல்படும். வைரஸ் காட்ஸ் (Virus Guards) என்பது காவலர்கள் போன்று உங்கள் கணினியை தொடர்ந்து கண்காணிக்கும். தீங்கிழைக்கும் மென்பொருளைக் கண்டறிவதுடன் அவை செயல்படவிடாமல் தடுக்கிறது. புதிய அச்சுறுத்தல் அணுகலைத் தடுப்பதற்கும், கண்டறியப்பட்ட அச்சுறுத்தல்களை அகற்றுவதற்கும் ∴பயர்வால்கள் பாதுகாப்பு பொறிமுறையை இயக்குகின்றன. வைரஸ் தடுப்பு மென்பொருள் இருந்தாலும் இணைப்புகளைத் தவிர்ப்பதன் மூலம் இணையத்தை எச்சரிக்கையுடன் பயன்படுத்துவது முக்கியம். விசேடமாக வணிக நடவடிக்கைகளுடன் தொடர்புபட்ட அரசாங்க நிறுவனங்கள் முக்கியத் தரவைப் பாதுகாத்துக் கொள்வதன் முக்கியமாவது ஏன் என்றால் இது அவர்களின் நற்பெயரை முன்னெடுப்பதற்கு ஒரு காரணமாகும் என்பதினாலேயே யாகும். வைரஸ் Virus Guards என்ற பொறி முறையிலான காவலர்கள் ஆவதுடன், நாளாந்தம் வளர்ச்சிக் கண்டுவரும் டிஜிட்டல் கட்டமைப்பில் உங்கள் சாதனங்கள் மற்றும் தரவைப் பாதுகாக்கும் இயந்திரக் காவலர்கள் என்று சுருக்கமாக கூறலாம்

SRI LANKA CERT|CC
Sri Lanka Computer Emergency Readiness Team
Coordination Centre

Risk

பாதுகாப்பற்ற தரவு சேமிப்பு மற்றும் மென்பொருளைப் பயன்படுத்துவதால் ஏற்படும் பாதிப்புகள்

டிஜிட்டல் வசதிகளை அனுபவிக்கும் நீங்கள் கண்டிப்பாக தரவு பரிமாற்றத்திற்காக வெளிப்புற தரவு சேமிப்பக வன்பொருளை பயன்படுத்தலாம். இருப்பினும், இதனால் ஏற்படக் கூடிய பாதிப்பு தொடர்பில் நீங்கள் கவனம் செலுத்த வேண்டியது முக்கியமாகும்.

வெளிப்புற சேமிப்பக வன்பொருள் இயக்கிகள் அதிக அளவிலான தரவை நகர்த்துவதற்கு வசதியாக இருந்தாலும், அவை உங்கள் மென்பொருள் மற்றும் தரவுகளை சேதப்படுத்துவதற்கான வாய்ப்புகள் கூடுதலாகவே உண்டு. இந்த வெளிப்புற தரவு சேமிப்பக ஹார்ட் டிரைவ்களை உங்கள் கணினிகளுடன் இணைக்கும் போது, அவற்றின் பரவலான பயன்பாடு, நமது கவனத்தை கோரும் உள்ளார்ந்த பாதிப்புக்களுடன் இடம்பெறக்கூடும்.

பொதுவான பாதிப்புக்கள்

தீங்கிழைக்கும் Malware மென்பொருள் ஊடாக பாதிக்கப்பட்ட வெளிப்புற தரவு சேமிப்பு வன்பொருள் இயக்கிகள் வைரஸ்கள், Ransomware அல்லது ஸ்பைவேர் Spyware ஒரு சாதனத்திலிருந்து மற்றொரு சாதனத்திற்கு பரவி, குறிப்பிடத்தக்க சேதத்தை ஏற்படுத்தும்.

தரவுகளை களவாடுதல்

உங்கள் ஹார்ட் டிரைவின் இழப்பு அல்லது திருட்டு உங்கள் ரகசியத் தரவை வேறொருவரினால் எளிதாக பெற்றுக்கொள்ள வழி வகுக்கும். இதன் மூவம் உங்கள் தனிப்பட்ட தகவல் அல்லது வணிக தகவலின் இரகசியத்தன்மையை இழக்க நேரிடலாம்.

பாதிப்புகளை குறைத்துக் கொள்ளல்

பாதிப்புகளை குறைத்துக் கொள்ளுவதற்காக உங்களுக்கு நம்பிக்கையான மற்றும் தரத்தைக்கொண்ட வெளி தரவு நிலையான வெளிப்புற சேமிப்பக வன்பொருளை மட்டுமே பயன்படுத்தவும். வைரசுகள் மற்றும் பழைய வைரஸ்களை எப்போதும் ஸ்கேன் செய்யவும். வெளிப்புற சேமிப்பக வன்பொருளைப் பாதுகாப்பாக வைத்திருப்பதற்கு, அதில் உள்ள முக்கியத் தரவை Encrypt (குறியீட்டுச்சொற்களால் மறைத்தல்) செய்வதிலும் கவனம் செலுத்த வேண்டும். இதுதொடர்பில் ஊழியர்கள் அல்லது குடும்ப உறுப்பினர்களிடையே பாதுகாப்பு விழிப்புணர்வை ஊக்குவிக்க வேண்டும். எச்சரிக்கையுடன் செயல்படுவதன் மூலமும், பாதுகாப்பான பயன்பாட்டு நடைமுறைகளைப் பின்பற்றுவதன் மூலமும், உங்கள் டிஜிட்டல் சாதனங்களுடன் தொடர்புடைய பாதிப்புகளை குறைத்துக்கொள்ளலாம்.

Protect

இணைய (Cyberspace) உலகில் தரவுகளை ரகசியமாக Privacy பாதுகாப்பது எவ்வாறு

- உங்கள் மின்னஞ்சல் மற்றும் பிற தொடர்புத் தகவலைப் பகிரங்கமாகப் பகிர்வதைத் தவிர்க்கவும்.தொலைபேசி எண்கள் உட்பட உங்கள் சமூக ஊடக கணக்குகளின் அமைப்புகளையும், புகைப்படங்கள் போன்ற உங்கள் தனிப்பட்ட தகவலை யார் பார்க்கலாம் என்பதை மறுசீராய்வு செய்யவும். நண்பர்கள் மட்டுமே இந்த தகவலை அணுக முடியும் என்பதை உறுதிப்படுத்துங்கள்.
- அனைவருக்கும் பொருந்தாத புகைப்படங்கள் அல்லது பிற உள்ளடக்கத்தைப் பகிரும் போது எச்சரிக்கையுடன் செயல்பட வேண்டும்.
- எல்வோரும் பார்க்க விரும்பாத புகைப்படங்கள் அல்லது பிற உள்ளடக்கங்களில் குறிப்பாக கவனமாக செயல்பட வேண்டும்.
- மற்றவர்களைப் பற்றிய தகவல்களைப் பகிரும் போது அவதானத்துடன் செயல்படுங்கள். உங்கள் நண்பர்கள் மற்றும் குடும்பத்தினரின் புகைப்படங்களை முழுமையாக அந்நியர்களுடன் பகிர்ந்து கொண்டால் - அதைப் பற்றி அவர்கள் எப்படி உணருவார்கள் என்பதை கற்பனை செய்து பாருங்கள்.
- உங்கள் சமூக ஊடக இடுகைகள் மற்றும் பகிர்வுகளில் பிரதிபலிக்கும் உங்கள் இணைய வழி ஆளுமை குறித்து கவனமாக செயல்பட வேண்டும். தொழிலுக்காக உங்களை மதிப்பிடும்போது, சாத்தியமான முதலாளிகள் உங்கள் இணைய இருப்பை ஆராயலாம் என்பதை கற்பனை செய்து பாருங்கள்.
- இணையவழி வினாடி வினா மற்றும் போட்டிகளில் ஈடுபடும் போது எச்சரிக்கையாக இருக்க வேண்டும். இதில் கலந்துகொள்பவர்கள் பொழுதுபோக்காகத் தோன்றினாலும், அவர்கள் உங்களைப் பற்றிய தகவல்களைச் சேகரிப்பதைக் கவனத்தில் கொள்வது அவசியம். உங்கள் ஆர்வங்கள் உட்பட அனைத்தும் இலாப நோக்கத்துடன் அவற்றை சந்தைப்படுத்தும் நிறுவனங்களுக்கு விற்கப்படலாம்.
- உங்களுக்குச் சொந்தமில்லாத கணினியை பயன்படுத்தும் போது மேம்பட்ட பாதுகாப்பிற்காக நன்னம்பிக்கையானவற்றையே தெரிவு செய்ய வேண்டும்.
- உங்களுக்கு தேவையானவற்றை பதிவிறக்கும் போது, அதற்கான அனுமதிகளை வழங்குவதற்கு முன், உங்கள் இருப்பிடம், முகவரி, புகைப்படங்கள், வீடியோக்கள் போன்றவற்றுக்கான அணுகல் அவர்களுக்கு உண்மையிலேயே தேவையா என்பதை கவனமாக மதிப்பீடு செய்துக்கொள்வது அவசியம்.
- நீங்கள் ஏதேனும் சந்தர்ப்பத்தில் தவறான படங்கள் அல்லது செய்திகளைப் பெற்றால், அவற்றின் திரை புகைப்படத்தை (Screenshot) எடுத்து அது தொடர்பில் சம்பந்தப்பட்ட பிரிவுக்கு முறைப்படு செய்ய முடியும்.

Global

அமெரிக்காவில் இணைய உலக (Cybersecurity) பாதுகாப்பு விழிப்புணர்வு மாதம்

எண்ணியல் (Digital) தொழில் நுட்பத்தை பயன்படுத்துவோர் மத்தியில் டிஜிட்டல் குற்றங்களில் இருந்து பாதுகாத்துக்கொள்வதற்கான விழிப்புணர்வை ஏற்படுத்துவதற்காக, இணைய பாதுகாப்பு Cybersecurity Awareness விழிப்புணர்வு மாதம் நடைமுறையில் இருந்துவருகிறது.

டிஜிட்டல் தொழில் நுட்பத்தை பயன்படுத்துவோர் டிஜிட்டல் வடிவ குற்றங்களில் தனிப்பட்ட தரவைப் பாதுகாக்க அனைவருக்கும் வசதி செய்யும் வகையில் அரசு மற்றும் தனியார் தொழில்துறைக்கு இடையிலான ஒரு கூட்டு முயற்சியாக தற்போது அமெரிக்காவில் இந்த திட்ட நிகழ்வுகள் மேற்கொள்ளப்பட்டுவருகின்றன.

இதன் கீழ் இணைய உலக பாதுகாப்பு முகவர் நிலையம் மற்றும் (CISA) நெஷனல், சைபர் செக்யூரிட்டி அலையன்ஸ் என்ற பங்குதாரர் நிறுவனங்கள் தங்கள் பணியாளர்கள் மற்றும் வாடிக்கையாளர்கள் இணையதளத்தை பாதுகாப்பாக பயன்படுத்துவதற்கான கலந்துரையாடுவதற்கென ஆதாரங்களுடன் தகவல் தொடர்புகளையும் உருவாக்குகின்றன. பெரும்பாலான இணைய பாதுகாப்பு செய்திக் கட்டுரைகள் பாரிய தரவு மீறல்களை உள்ளடக்கியதாக அமைந்துள்ளன. ஹெக்கர்கள், மிகப்பெரியதாகத் தோன்றலாம் மற்றும் அதற்கு எதிராக நீங்கள் சக்தியற்றவர் போல் இருப்பதாகக்கூட உணரலாம். ஆனால் சைபர் செக்யூரிட்டி விழிப்புணர்வு மாத நிகழ்வில் உங்களது தரவுகளை பாதுகாப்பதற்கான வழி முறைகள் குறித்து விளக்கமளிக்கப்படுகிறது. இணையப் பாதுகாப்பின் அடிப்படைகளைப் பயிற்சி செய்வதன் மூலம் இது ஒரு பெரிய மாற்றத்தை ஏற்படுத்த முடியும் என்பது குறிப்பிடத்தக்கது.

இந்தவருடத்தில் பொதுமக்கள் விழிப்புணர்வை ஏற்படுத்தும் திட்ட நிகழ்வில் பின்வரும் விடயங்கள் தொடர்பில் கவனம் செலுத்த தீர்மானித்துள்ளனர்.

- வலுவான கடவுச் சொற்களையும், கடவுச்சொல் நிர்வாக செயற்பாட்டை மேற்கொள்ளல் Use strong passwords and a password manager
- பல காரணி உறுதிப்படுத்தல் முறையை மேற்கொள்ளல் Turn on multifactor authentication
- சமூக பொறியியல் பொறிமுறையை அடையாளங் கண்டு முறைப்பாடு செய்தல் Recognize and report phishing
- மென்பொருளை மேம்படுத்துவது முக்கியமாகும் Update software

Published By
CERT Media