வெளியீடு 02

Cyber Guardian

2024

Publication for your online safety

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

இணைய பாதுகாப்பு குறித்து அரசு அதிகாரிகளுக்கு பயிற்சி அளிப்பதில் தனியார் துறைக்கு ஆதரவளிக்கவும்

இலங்கை CERT ஆனது இலங்கை தகவல் தொழில்நுட்ப தொழிற்சங்க சம்மேளனம் (FITIS) மற்றும் ISC2 கொழும்பு அத்தியாயத்துடன் ஒரு அற்புதமான பயணத்தை மேற்கொள்கிறது, ஏப்ரல் 3 ஆம் திகதி SLIDA இல் ஒரு முக்கியமான புரிந்துணர்வு ஒப்பந்தத்தில் கையெழுத்திடப்பட்டது. இந்த தொலைநோக்கு ஒத்துழைப்பு அடுத்த இரண்டு ஆண்டுகளில் 1,000 அரசாங்க அதிகாரிகளுக்கு வழிகாட்டுதல் மற்றும் பயிற்சி அளிப்பதற்கும், அரசாங்க நிறுவனங்கள் மற்றும் பரந்த விநியோகச் சங்கிலி சுற்றுச்சூழலுக்குள்ளும் இணையப் பாதுகாப்புத் திறனை மேம்படுத்துவதற்கும் களத்தை அமைக்கிறது.

எப்போதும் வளரும் டிஜிட்டல் நிலப்பரப்பில்,ஒத்துழைப்பு வெற்றிக்கான திறவுகோலாக வெளிப்படுகிறது. இலங்கை தகவல் தொழில்நுட்ப தொழிற்சங்க சம்மேளனம் (FITIS) மற்றும் ISC2 கொழும்பு அத்தியாயம் ஆகியவற்றுடனான எங்கள் கூட்டாண்மை மூலம், புதுமை, அறிவுப் பரிமாற்றம் மற்றும் கூட்டு வலுவூட்டல் ஆகியவற்றின் கலாச்சாரத்தை நாங்கள் உயர்த்துகிறோம். இந்த புரிந்துணர்வு ஒப்பந்தம் இணையப் பாதுகாப்புக் கல்வியை மேம்படுத்துதல், விழிப்புணர்வை அதிகரிப்பது மற்றும் தொழில்முறை வளர்ச்சியை வளர்ப்பதில் எங்களின் உறுதிப்பாட்டை அடிக்கோடிட்டுக் காட்டுகிறது. ஒன்றாக, டிஜிட்டல் டொமைனின் சிக்கல்களை நம்பிக்கையுடனும் நெகிழ்ச்சியுடனும் வழிநடத்த, அரசாங்க அதிகாரிகளுக்கும் சப்ளை செயின் பங்குதாரர்களுக்கும் அதிகாரம் அளிப்போம்.

கையொப்பமிடும் நிகழ்வில் கலந்துகொண்ட கௌரவ அதிதிகளான கௌரவ. கனக ஹேரத், தொழில்நுட்ப இராஜாங்க அமைச்சர், கலாநிதி தர்மஸ்ரீ குமாரதுங்க, தொழில்நுட்ப அமைச்சின் செயலாளர் திரு.நாலக களுவெவ, ளுடுஜனுயு இன் பணிப்பாளர் நாயகம், இலங்கைக்கான அமெரிக்கத் தூதரகத்திலிருந்து திரு.அன்ட்ரூ ஷின், திரு. ஜனக சம்பத் - இலங்கை CERT தலைவர் (Actg), CEO (Actg) Dr. கனிஷ்க கருணாசேன, FITIS இன் தலைவர் திரு. இந்திக டி சொய்சா மற்றும் ISC2 கொழும்பு பிரிவின் தலைவர் திரு. சுஜித் கிறிஸ்டி. FITIS இன் பிரதம நிறைவேற்று அதிகாரி திரு. ஜெயசிறி அமரசேன.

Policy//

உத்தியோகபூர்வ வேலைக்கான தனிப்பட்ட சாதனங்களைப் பயன்படுத்துவதற்கான கொள்கை

உத்தியோகபூர்வ கடமைகளை நிறைவேற்ற பணியாளர்கள் தங்கள் தனிப்பட்ட மடிக்கணினிகள், ஸ்மார்ட்போன்கள் மற்றும் tabs பயன்படுத்த நிறுவனம் அனுமதிக்காது. இருப்பினும், ISC ஆல் நிர்ணயிக்கப்பட்ட குறிப்பிட்ட சூழ்நிலையில், ISO இன் மேற்பார்வையின் கீழ், உத்தியோகபூர்வ கடமைகளைச் செய்ய, தேர்ந்தெடுக்கப்பட்ட பணியாளர்கள் தங்கள் தனிப்பட்ட சாதனங்களைப் பயன்படுத்த அமைப்பு அனுமதிக்கலாம். இதுபோன்ற சூழ்நிலைகளில், அத்தகைய சாதனங்களை நிறுவனத்துடன் சரியான முறையில் பதிவுசெய்து, அந்த சாதனங்கள் இந்தக் கொள்கையுடன் இணங்குகின்றனவா என்பதை உறுதிப்படுத்துவது அவசியம் ஆகும்.

எவ்வாறாயினும், எந்தவொரு சூழ்நிலையிலும் "ரகசியம்" மற்றும் "மறைவான" என வகைப்படுத்தப்பட்ட தகவலைச் செயலாக்கவோ அல்லது சேமிக்கவோ பணியாளர்களின் தனிப்பட்ட சாதனங்கள் பயன்படுத்தப்படமாட்டாது.

உத்தியோகபூர்வ கடமைகளைச் செய்ய ஊழியர்களின் தனிப்பட்ட சாதனங்கள் பயன்படுத்தப்படும் போது, பயனர் கணக்குகள் வரையறுக்கப்பட்ட சலுகைகளுடன் அமைக்கப்படுவதையும், வலுவான கடவுச்சொற்கள் மற்றும் Multifactour அங்கீகாரத்துடன் கணக்குகள் பாதுகாக்கப்படுவதையும், Malware மென்பொருள் நிறுவப்பட்டு, Auto Updateகள் இயக்கப்பட்டிருப்பதையும் நிறுவனம் உறுதி செய்யும். பயன்பாட்டு மென்பொருள் மற்றும் பயன்படுத்தப்படும் பிற பயன்பாட்டு மென்பொருள்கள் தேவையான Patch புதுப்பிப்புகளுடன் செல்லுபடியாகும் உரிமங்களைக் கொண்டுள்ளனவா என்பதையும் நிறுவனம் உறுதி செய்யும்.தடயவியல் விசாரணையின் போது,கடமை நோக்கங்களுக்காகப் பயன்படுத்தப்படும் தனிப்பட்ட சாதனங்களில் தனிப்பட்ட மற்றும் நிறுவனத் தகவல்களை விசாரிக்க அல்லது விசாரணை நோக்கங்களுக்காக அத்தகைய சாதனங்களைத் தக்கவைத்து, சட்டத் தேவைகளின் பேரில் அவற்றை அரசாங்க முகவர் அல்லது கட்சிகளுக்கு விடுவிப்பதற்கான உரிமையை நிறுவனம் கொண்டுள்ளது.

தனிப்பட்ட சாதனத்தின் பாதுகாப்பு சாதனத்தின் உரிமையாளரின் பொறுப்பாகும். சாதனத்தைப் பயன்படுத்துவதால் தனிப்பட்ட தரவு இழப்பு உட்பட சாதனத்திற்கு ஏற்படும் இழப்பு அல்லது சேதத்திற்கு நிறுவனம் பொறுப்பேற்காது

இணக்கம்: அனைத்து அரசு நிறுவனங்களுக்கும் பொருந்தும்

சைபர் செக்யூரிட்டியில் பயிற்சி முடித்த அரசு அதிகாரிகள் மற்றும் பத்திரிகையாளர்களுக்கு சான்றிதழ்கள் வழங்கப்பட்டன.

தலைமை தகவல் தொழில்நுட்ப அதிகாரிகளுக்கான இலங்கை செர்ட் நிறுவனம் ஏற்பாடு செய்த இணைய பாதுகாப்பு பயிற்சி நெறியில், அரச நிறுவனங்களின் உதவி தகவல் தொழில்நுட்ப அதிகாரிகள் (ISO/AISO) ஆகி அதிகாரிகள் பங்குபற்றினர். 37 அரசு நிறுவனங்களைச் சேர்ந்த 60 அதிகாரிகள் விழாவில் கலந்து கொண்டனர். மேலும், இணைய பாதுகாப்பு மற்றும் இணைய பாதுகாப்பு சம்பவங்களை பொதுமக்களுக்கு திறம்பட புகாரளிப்பது குறித்து பத்திரிக்கையாளர்களுக்கு கல்வி அளிக்கப்பட்டது. இந்நிகழ்ச்சியில் கலந்து கொண்ட நாற்பது ஊடகவியலாளர்களும் சான்றிதழ்களைப் பெற்றனர். தொழில்நுட்ப இராஜாங்க அமைச்சர் திரு கனக ஹேரத் பிரதம அதிதியாக கலந்து கொண்டு சான்றிதழ் வழங்கும் நிகழ்வு SLIDA இல் இடம்பெற்றது. கலந்துகொண்டவர்களில், தொழில்நுட்ப அமைச்சின் செயலாளர் கலாநிதி தர்மஸ்ரீ குமாரதுங்க, SLIDA இன் பணிப்பாளர் நாயகம் நாலக களுவெவ, இலங்கைக்கான அமெரிக்க தூதரகத்தைச் சேர்ந்த அன்ட்ரூ ஷின், இலங்கை செர்ட்டின் பதில் தலைவர் ஜானக சம்பத், Sri Lanka Cert இன் CEO கலாநிதி கனிஷ்க கருணாசேன, FITIS இன் தலைவர் இந்திக்க டி சொய்சா மற்றும் ISC2 கொழும்பு பிரிவின் தலைவர் திரு. சுஜித் கிறிஸ்டி ஆகியோர் கலந்துகொண்டனர்.

சைபர் பாதுகாப்பிற்கு AI ஒரு அச்சுறுத்தலா?

வாடிக்கையாளர்கள் தங்கள் அன்றாட வாழ்வில் AI கருவிகளை ஒருங்கிணைக்கும்போது, உணவை நிர்வகிப்பது முதல் மருத்துவ ஆலோசனை பெறுவது வரை, பாதுகாப்பு மற்றும் மோசடி அபாயங்கள் பற்றிய கவலைகள் எழுகின்றன. "KPMG ஆய்வு அறிக்கையின் அடிப்படையில் தகவல் பாதுகாப்பு இதழின் கண்டுபிடிப்புகள், நன்கு செயல்படுத்தப்பட்ட AI பயன்பாடுகளில் கூட சாத்தியமான பாதிப்புகளை எடுத்துக்காட்டுகின்றன. நுகர்வோர் இந்த அமைப்புகளில் முக்கியமான தகவல்களை விருப்பத்துடன் உள்ளீடு செய்து, தங்களைத் தீங்கு விளைவிக்கக் கூடிய சாத்தியக்கூறுகளை வெளிப்படுத்துகின்றனர். இது தனிநபர்களை ஆபத்தில் ஆழ்த்துவது மட்டுமல்லாமல் வணிகங்கள் மற்றும் ஒட்டுமொத்த இணையப் பாதுகாப்பு நெறிமுறைகளையும் பாதிக்கிறது.

நுகர்வோரில் கணிசமான பகுதியினர், AI கருவிகளைப் பயன்படுத்தும் போது, பெரும்பாலும் பின்விளைவுகளைக் கருத்தில் கொள்ளாமல், அபாயகரமான நடத்தையில் ஈடுபடுவதாக கணக்கெடுப்பு சுட்டிக்காட்டுகிறது. மூன்றில் ஒரு பகுதியினர் (38%) நிதித் தகவலை உள்ளிடுவதை ஒப்புக்கொள்கிறார்கள், அதே நேரத்தில் 27% பேர் முகவரிகள் அல்லது பிறந்த திகதி போன்ற தனிப்பட்ட விவரங்களை வெளியிடுகின்றனர். அடையாள திருட்டு, நிதி மோசடி மற்றும் பிற மோசமான நடவடிக்கைகளுக்கு சைபர் குற்றவாளிகளுக்கு இத்தகைய தரவு விலைமதிப்பற்றது.

நுகர்வோரில் கணிசமான பகுதியினர், AI கருவிகளைப் பயன்படுத்தும் போது, பெரும்பாலும் பின்விளைவுகளைக் கருத்தில் கொள்ளாமல், அபாயகரமான நடத்தையில் ஈடுபடுவதாக கணக்கெடுப்பு சுட்டிக்காட்டுகிறது. மூன்றில் ஒரு பகுதியினர் (38%) நிதித் தகவலை உள்ளிடுவதை ஒப்புக்கொள்கிறார்கள், அதே நேரத்தில் 27% பேர் முகவரிகள் அல்லது பிறந்த திகதி போன்ற தனிப்பட்ட விவரங்களை வெளியிடுகின்றனர். அடையாள திருட்டு, நிதி மோசடி மற்றும் பிற மோசமான நடவடிக்கைகளுக்கு சைபர் குற்றவாளிகளுக்கு இத்தகைய தரவு விலைமதிப்பற்றது.

சைபர் கிரைமினல்கள் ஏற்கனவே தங்கள் தாக்குதல் முறைகளை மேம்படுத்த அளவிடக்கூடிய AI கருவிகளைப் பயன்படுத்துகின்றனர். ரகசியத் தகவலைப் பகிர்ந்து கொள்வதற்கான நுகர்வோர் விருப்பம் இந்த அச்சுறுத்தலை அதிகப்படுத்துகிறது. deep fake AI போன்ற வளர்ந்து வரும் அபாயங்களுடன் இணைந்து, டிஜிட்டல் நிலப்பரப்பு வஞ்சக தாக்குதல்களுக்கு அதிக பாதிப்பை எதிர்கொள்கிறது.

பெரும்பாலான பயனர்கள் (59%) தொழில்நுட்பத்தைப் பற்றி தங்களை அறிந்தவர்களாகக் கருதினாலும், பலர் இன்னும் ஆபத்தான மோசடிகளுக்கு இரையாகிறார்கள். இதுபோன்ற சம்பவங்களுக்கு நுகர்வோரை குற்றம் சாட்டுவது சாதாரணமாகிவிட்டது, இருப்பினும் நிதிச் சேவைகள் (25%), சுகாதாரம் (18%), மற்றும் அரசு (15%) போன்ற துறைகள் கடுமையான விதிமுறைகளுக்கு வாதிடுகின்றன. ஏறக்குறைய 20% அனைத்து துறைகளும் ஒரே தரநிலையை கடைபிடிக்க வேண்டும் என்று நம்புகின்றனர். இருப்பினும், ஆபத்துக்களைத் தணிக்க விழிப்புணர்வுடன் டிஜிட்டல் தொழில்நுட்பங்களைப் பயன்படுத்துவதில் நுகர்வோரும் பொறுப்பேற்கிறார்கள்."