September 2022 New Zealand Information Security Manual v3.6 Release

Change Area: Public Cloud Security (New Chapter)

Rationale:

In July 2016, Cabinet agreed that agencies can also use public cloud to deliver office productivity services, provided they comply with security guidance issued by the GCDO and the GCSB, but the NZISM has not provided any detailed guidance on this.

Change Description:

A new chapter has been written which will provide information security guidance on key security concepts and architecture patterns related to public cloud services.

Topics included in this chapter cover: An introduction to Public Cloud Security Concepts; Governance, Risk and Assurance; Identity Management and Access control; Data Protection; Logging and Alerting.

Expected Outcome:

Agencies understand key concepts and implement controls related to securing their use of public cloud services.

New Security Controls		Modified Security Controls		Rescinded Security Controls	
Control	CID	Control	CID	Control	CID
23.1.54.C.01	7349				
23.1.54.C.02	7350				
23.1.55.C.01	7353				
23.1.55.C.02	7354				
23.1.55.C.03	7355				
23.1.56.C.01	7359				
23.2.16.C.01	7386				
23.2.16.C.02	7387				
23.2.16.C.03	7388				
23.2.16.C.04	7389				
23.2.17.C.01	7394				
23.2.18.C.01	7397				
23.2.19.C.01	7400				
23.2.20.C.01	7404				
23.2.21.C.01	7407				
23.3.18.C.01	7433				
23.3.19.C.01	7436				
23.3.19.C.02	7437				
23.3.20.C.01	7440				
23.3.21.C.01	7443				
23.3.22.C.01	7446				
23.4.9.C.01	7461				

23.4.9.C.02	7462				
23.4.9.C.03	7463				
23.4.10.C.01	7466				
23.4.11.C.01	7469				
23.4.11.C.02	7470				
23.4.12.C.01	7474				
23.4.12.C.02	7475				
23.4.13.C.01	7511				
23.4.13.C.02	7512				
23.4.13.C.03	7513				
23.5.10.C.01	7494				
23.5.11.C.01	7496				
23.5.12.C.01	7498				
23.5.12.C.02	7499				

Change Area: Inverse Split-Tunnel VPN (New Section)

Rationale:

Architecture advice advocates for the use of inverse split tunnelling, where an explicit list of authorised and trusted internet based services are able to be directly accessed, bypassing agency perimeter controls. Both the architecture advice, and the NZISM, advise against the use of full split tunnelling.

Change Description:

A new section on Inverse Split tunnelling has been written for Chapter 18 Network Security. This section covers information relating specifically to configuring secure remote access services (also known as VPN services) for agency devices that facilitate agency information (e.g. documents or emails) being transferred to remote systems.

Expected Outcome:

Agencies identify and effectively manage the risks and compensating controls involved in utilising inverse split tunnelling as part of remote access virtual private network (VPN) configurations.

New Security Controls		Modified Security Controls		Rescinded Security Controls	
Control	CID	Control	CID	Control	CID
18.7.14.C.01	7250				
18.7.14.C.02	7251				

Change Area: Language Modernisation (Whole NZISM)

Rationale:

A survey of international national cybersecurity centres, standards associations, professional associations, and private companies shows broad consensus to update terminology. A current NZ survey shows the NZ public does not accept language which perpetuates racism.

Change Description:

There are a number of computing terms that should be avoided in professional writing, since they are not strictly needed and are considered offensive or exclusionary by some groups. In this release whitelist, blacklist, and man-in-the-middle have been updated; other terms will be updated in future releases.

Expected Outcome:

The NCSC encourages New Zealand organisations to adopt and normalise these new terms.

The following are controls that have had editorial changes:

New Security Controls		Modified Security Controls		Rescinded Security Controls	
Control	CID	Control	CID	Control	CID
		12.4.5.C.01	3455		
		14.2.4.C.01 14.2.5.C.01 14.2.5.C.04 14.2.6.C.01 14.2.7.C.02 14.2.7.C.03 14.2.7.C.05 14.2.7.C.07	1234 1242 898 907 936 940 945 947		
		14.3.8.C.01 14.3.10.C.01 14.3.10.C.02 14.3.10.C.03 14.3.10.C.04	1602 1609 1608 1610 1611		
		15.2.23.C.01			
		18.3.12.C.01 18.3.12.C.02	3740 3741		
		19.5.28.C.05	4752		
		20.3.12.C.01 20.3.12.C.02	4406 4407		

Change Area: DMARC (Domain-based Message Authentication, Reporting and Conformance); DKIM (DomainKeys Identified Mail) (Update to section 15.2)

Rationale:

Phishing and malware distribution attacks are common internet security threats. To limit the possibility of agency domains being used fraudulently (e.g. for spam or spear-phishing), agencies should implement: a Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM); and Domain-based Message Authentication, Reporting & Conformance (DMARC) records.

Agencies have had some time to start implementing the full provisions of DMARC/DKIM and it was always the intention of the NZISM to change these to MUST controls. The future replacement for SEEMail will use DMARC and therefore vendors and agencies will need to be compliant.

Change Description:

1. Change of DMARC control compliance from SHOULD to MUST [CID:6019] [CID:6021]

2. Change of DMARC policy setting from p="none" to p="reject" [CID:6020]

3. Change of DKIM control compliance from SHOULD to MUST [CID:1797] [CID:1798]

Expected Outcome:

A reduction in the number of Government email domains being used for spam or email phishing campaigns.

New controls		Modified security controls			Renumbered controls		
Control	CID	Old control	CID	New control	Old control	CID	New control
		15.2.22.C.01	6019	15.2.20.C.01			
		15.2.22.C.02	6020	15.2.20.C.02			
15.2.20.C.03	7519						
		15.2.22.C.03	6021	15.2.20.C.04			
15.2.20.C.05	7520						
		15.2.23.C.01	1745	15.2.21.C.01			
					15.2.24.C.01	1749	15.2.22.C.01
					15.2.25.C.01	1754	15.2.23.C.01
					15.2.25.C.02	1755	15.2.23.C.02
					15.2.25.C.03	1756	15.2.23.C.03
					15.2.26.C.01	1760	15.2.24.C.01
					15.2.26.C.02	1761	15.2.24.C.02
					15.2.27.C.01	1764	15.2.25.C.01
					15.2.27.C.02	1765	15.2.25.C.01
		15.2.28.C.01	1768	15.2.26.C.01			
					15.2.29.C.01	1771	15.2.27.C.01
		15.2.30.C.01	1774	15.2.28.C.01			
					15.2.31.C.01	1777	15.2.29.C.01
					15.2.32.C.01	1780	15.2.30.C.01

					15.2.32.C.02	1781	15.2.30.C.02
					15.2.32.C.03	1782	15.2.30.C.03
					15.2.33.C.01	1786	15.2.31.C.01
					15.2.33.C.02	1787	15.2.31.C.02
					15.2.34.C.01	1792	15.2.32.C.01
		15.2.34.C.02	1793	15.2.32.C.02			
		15.2.34.C.03	1794	15.2.32.C.03			
		15.2.35.C.01	1798	15.2.33.C.01			
		15.2.35.C.02	1797	15.2.33.C.02			
					15.2.35.C.03	1799	15.2.33.C.03
					15.2.35.C.04	1800	15.2.33.C.04

Change Area: Chapter 9. Section 9.2. Authorisations, Security Clearances and Briefings

New Security Controls		Modified Security Controls		Rescinded Security Controls	
Control	CID	Control	CID	Control	CID
		9.2.11.C.02	1484		
		9.2.12.C.01	1487		
		9.2.18.C.01	1508		