Advanced Corporate Solutions

TSCM | "Debugging" Specialists | Service Excellence since 1995

dynamdre

INNOVATIVE SOLUTIONS

Information Security I www.dynamdre.co.za

WC Aug 2020

SMART HOMES

Protecting Company Owned Data at Home

"HOME IS WHERE THE WiFi ALWAYS CONNECTS"

A school girl once said: “We only need food, transport, and WiFi”.

This cannot be more true. With current state of COVID-19 lock-down, families are forced to work from home. This now creates an environment where data from different companies are processed on devices, that are pen-ultimately connected to the same home WiFi infrastructure. This raises the question "How secure are your home networks?"

The need for Smart home automation and devices are booming. Technologists calls it Internet of Things, or the next Industrial revolution. Simply put, it boils down to bringing various devices into your home, to make your life easy. All these devices connect to your home WiFi infrastructure, and yet most of these devices are manufactured in foreign countries with questionable privacy laws.

Do we truly understand the functionality of these devices? Do we truly understand how these devices process, share or relay information? Do we truly understand the key security configuration requirements, needed to ensure information security on these devices?

SMART HOMES

The Risks Involved

"Two out of five smart households are vulnerable to cyber attacks according to new research.It only takes one vulnerable device to compromise the security of an entire home network and the research clearly illustrates the danger posed by unsecured Internet of Things (IoT) devices.

The majority (69.2%) of vulnerable devices in smart homes worldwide were discovered to be susceptible to attacks due to having weak credentials in the form of simple passwords or only using one-factor authentication. An additional 31.8 percent of these devices worldwide were vulnerable as a result of not being patched. Out-of-date software is often the weakest link in the security chain, providing cyber criminals with an easy way to gain access to consumer devices and their home networks.

People use their smart TV to watch their favorite Netflix series or connect their baby monitor to their home network, however often they don't know how to maintain their devices' security. It only takes one weak device to let in a bad hacker and once they are on the network, they can access other devices, and the confidential data they stream or store, including live videos and voice recordings. Simple security steps like setting strong, unique passwords and two-factor authentication for all device access, and ensuring software patches and firmware updates are applied when available, will significantly improve digital home integrity.

SMART HOMES

Our Risk Assessment Services

ACS in conjunction with Dynamdre can assist you with our proactive risk assessment services:

1. TSCM / "Debugging" Sweeps / Assessments - Skilled TSCM / "Debugging" assessments needs to be conducted on a regular basis, at least once a month.
2. Vulnerability Assessments - Vulnerability assessments across all your devices, preferably every second month.
3. Remediation Planning and Reporting - Vulnerabilities, uncovered during these assessments, should be classified in accordance to their severity, and fixed accordingly.
4. If you are unsure, or need guidance, contact the specialists - our expertise are but a phone call away. Contact us today and find out how we can assist you in improving your information security posture, and safeguard your intellectual property.

Advanced Corporate Solutions
TSCM | "Debugging" Specialists | Service Excellence since 1995

dynamdre
INNOVATIVE SOLUTIONS
Information Security I www.dynamdre.co.za

Riaan Bellingan (Snr)
Office: +27 (0) 12 349 1779
Cell: +27 (0) 82 491 5086
Email: riaan@acsolutions.co.za
Website: www.acsolutions.co.za

Riaan Bellingan (Jnr)
Office: +27 (0)12 880 2238
Cell: +27 (0) 72 671 5764
Email: riaan@dynamdre.co.za
Website: www.dynamdre.co.za