KERATAN AKHBAR-AKHBAR TEMPATAN
TARIKH: 7 JULAI 2017 (JUMAAT)

Bil	Tajuk	Akhbar
1	MTDC jangka empat syarikat teknologi disenarai	Berita Harian
2	Are we prepared for cyber attacks?	The Star

KERATAN AKHBAR
BERITA HARIAN (BISNES) : MUKA SURAT B4
TARIKH: 7 JULAI 2017 (JUMAAT)

MTDC jangka empat syarikat teknologi disenarai

Malaysian Technology Development Corp Sdn Bhd (MTDC) menjangkakan sekurang-kurangnya empat syarikat teknologi akan disenaraikan di Bursa Malaysia menjelang 2018 dan 2020.

Ketua Pegawai Eksekutif, Datuk Norhalim Yunus, berkata syarikat berkenaan terbabit dalam bidang peranti perubatan, robotik dan bahan kimia.

"Dua daripada syarikat itu akan disenaraikan di pasaran ACE, manakala satu lagi mungkin dalam pasaran utama. Penyenaraian akan dibuat secara beransur-ansur menjelang 2020 kerana kami perlu mempersiapkan mereka untuk mendapat penilaian yang lebih baik," katanya.

Norhalim berkata demikian kepada pemberita pada dialog sulung mengenai penyenaraian merentas sempadan di Akademi Latihan Usahawan Teknologi MTDC (TENTRA) yang dibuat serentak dengan majlis sambutan Hari Raya di Serdang, semalam.

Wujud banyak tawaran

Sehingga sekarang, ekosistem pengkomersialan MTDC telah memberikan pembiayaan dan bantuan kepada lebih 500 syarikat yang berasaskan teknologi.

Sementara itu, Norhalim melihat pasaran 'Platform Pemecut Usahawan Peneraju' (LEAP) di Bursa Malaysia, sebagai satu peluang yang besar untuk membolehkan syarikat permulaan mengumpul dana bagi mengembangkan perniagaan mereka.

"Pada pandangan kami, sebagai pembiaya peringkat awal, ini adalah satu perkembangan yang sangat menarik kerana ia melengkapi apa yang kami sudah ada."

Beliau menjangkakan akan wujud lebih banyak tawaran untuk syarikat MTDC dengan LEAP memandangkan papan kedua itu memerlukan rekod sejarah.

"Ini adalah satu perubahan kepada ekosistem di mana sebelum ini, kami ada dana kerajaan yang membantu pada peringkat awal syarikat. Sekarang, kami mempunyai potensi untuk mendapatkan dana daripada pelabur yang berpengetahuan untuk melabur sejajar dengan perkembangan syarikat," katanya.

Dialog TENTRA semalam menyaksikan wakil Bioalpha Holdings Bhd, DagangHalal Plc, Green & Smart Plc, Axcelasia Inc dan Bursa Malaysia Bhd berkongsi pengalaman dan pandangan, masing-masing mengenai langkah penyenaraian mereka dahulu.

DagangHalal dan Green & Smart adalah dua syarikat penerima MTDC yang telah berjaya disenaraikan di pasaran kecil Bursa Saham London tahun lalu.

Axcelasia disenaraikan di Bursa Singapura dan Bioalpha Holdings di pasaran ACE Bursa Malaysia sejak tahun 2015. **BERNAMA**

Fakta nombor

500 SYARIKAT
MTDC beri pembiayaan dan bantuan berasaskan teknologi

KERATAN AKHBAR
THE STAR (NEWS STARBIZ) : MUKA SURAT 2
TARIKH: 7 JULAI 2017 (JUMAAT)

Are we prepared for cyber attacks?

Reflections
B.K. SIDHU
starbiz@thestar.com.my

GOING by the recent United Nations (UN) survey, Malaysia ranks third in terms of protecting itself against cyber attacks, ahead of more advanced nations.

Singapore tops the list, followed by the United States. The others on the top-10 list include Oman, Estonia, Mauritius, Australia, Georgia, France and Canada.

The UN's Global Cybersecurity Index 2017 released on Wednesday took a look at the defence capabilities of 134 countries, focusing on five factors: technical, organisational, legal, cooperation and growth potential, and also those "most committed" to cyber security.

But it did say there were evident gaps between countries in terms of awareness, understanding, knowledge and capacity to deploy the proper strategies, capabilities and programmes.

Another survey finding released yesterday by security services company Quann and research firm IDC showed that 96% of Malaysian companies were in the early stages of security preparedness.

While these companies recognise the importance of cyber security, most companies have only basic security features such as firewalls and antivirus protection. About half do not have proper security intelligence and event management systems in place to monitor and raise alerts for anomalies.

They also found that the weakest link in cyber security were the non-IT employees, but only 31% of companies want their employees to take part in IT security training.

These findings are similar for Hong Kong and Singapore. Over 150 security professionals from medium to large companies in Hong Kong, Singapore and Malaysia were surveyed.

The crux of the matter is that many companies are still not spending enough on IT security because to them, there is no visible returns on investment. But cyber security spending has to be treated like military spending – you need to be armed with the right tools to use in a war because cyber attacks are getting rampant.

Yesterday, Malaysian brokers were in for a surprise as there was a distributed denial-of-service, which lasted for two hours, causing some disruption.

As though May's WannaCry ransomware attack that shocked the world is not enough evidence that systems can be paralysed. WannaCry infected hundreds of computers in over 150 countries, paralysing hospitals in Spain and Britain, ravaging computers at universities in China, rail systems in Germany and even auto plants in Japan.

And the recent Petya outbreak has also sent shockwaves globally less than two months after WannaCry.

Whatever the ranking, cyber attacks will continue as the Internet is matured and hackers are getting more sophisticated.

The cyber war is out there, it is about being prepared and this is not just for companies. Individuals with machines are equally vulnerable to hacking and ransomware.

You may just be sitting in your favourite cafe and working on your laptop using public WiFi but this could pose a huge risk, as hackers have several ways to infiltrate these networks. Reports have said that they can just create their own public WiFi networks with names that are similar to your cafe and steal all your information.

There is a lot that needs to be done and frequent anti-virus and anti-malware software updates are necessary to avoid gaps in your cyber security.

Train your employees on proper updating protocols, make passwords stronger and turn off the WiFi on your devices when not in use. This is to prevent it from automatically connecting to available WiFi hotspots.