

THE CONVERSATION

Academic rigour, journalistic flair



DAN PELED/AAP

MyGov's ill-timed meltdown could have been avoided with 'elastic computing'

March 27, 2020 5.04pm AEDT

These past few weeks have shown the brittleness of Australia's online systems. It's not surprising the federal government's traditionally slow-moving IT systems are buckling under the pressure.

On Sunday, the federal government announced it would double unemployment benefits as part of its coronavirus rescue package. But when MyGov's online services crashed, thousands of desperate Australians felt compelled to disobey social distancing rules – forming long queues outside Centrelink offices across the country.

With widespread school and university closures, IT services are now the contingency plan of the education sector. For many, they're the main means of interacting with the outside world.

Unfortunately, these services are only as good as their design. And unless designers prepare for extreme circumstances such as this pandemic, they're destined to fail.

MyGov's failure outlined

This week, Australia's welfare system ground to a halt as thousands of people anxiously tried to register for promised federal government support.

Author



Erica Mealy

Lecturer in Computer Science, University of the Sunshine Coast

According to the 2016 census, the number of Australians working in hospitality makes up 6.9% of the population. Thus, we can estimate about 1.75 million people were affected by sector-wide hospitality service closures.

Economists estimate additional coronavirus measures to #flattenthecurve could see the unemployment rate double to more than 11%. This would represent 2.8 million Australians – more than 22 times the number of users MyGov can support at any one time.

Read more: The internet is surprisingly fragile, crashes thousands of times a year, and no one is making it stronger

As of Sunday evening, the online government portal (which people were directed to to access additional welfare) was able to cope with about 6,000 people at one time. This is a mere 0.3% of the expected number of Australians affected.

By mid-Monday, the amount of users MyGov could support increased to 55,000 or 3.1% of those affected. By Tuesday, this figure rose to 123,000 users, or 7.5%.

But why was the system poorly provisioned?

Having a large number of users access an online portal at once has many costs. Maintaining computer servers that allow this much load is expensive for any business, let alone a government facing the threat of an economic crisis.

The IT industry has solved this problem through cloud computing. This involves having a set of computers owned by companies such as Amazon or Google, and “renting” their storage and processing power as needed.

To understand this, think of Elton John on tour. He doesn't own stadiums in every city. When he needs to perform, he leases them as needed. He also selects a venue of the appropriate size, as needed.

The same concept applies in computing. The IT industry now has the capacity to rent appropriately-sized computing resources as needed. Furthermore, systems can be designed to automatically increase leased storage and processing power when required. This is called “elastic computing”.

Read more: Why we need to improve cloud computing's security

Had MyGov and Centerlink used elastic computing, the failures this week could have been prevented. Even the government's Secure Cloud Strategy doesn't mention using or supporting elastic computing strategies. This is despite last year's announcement that the Amazon AWS Cloud, which supports elastic computing, is the Australian government's cloud computing provider.

In terms of security, cloud computing providers arguably have better cybersecurity records than our federal government.

Denial of Service attacks

In 2016, the federal government showed exactly how poorly they understand users' needs. The online census was, in simple words, disastrous. Many people were unable to login to complete it, and from those who were, many had their session fail and logout prematurely.

But what caused #censusfail?

The system designers failed to anticipate everyone would login at once, on the same night. The number of users competing for access at one time (allowing for different time zones across the country) was up to a quarter of the population. Given Australia has about 25.4 million people, this means about 6.3 million people were trying to complete the census at the same time.

The system was not designed to cope. In computing, when a server has more users than it can service, the impact is the same as a Denial of Service (DoS) attack, in which normal traffic can't be processed. And a Denial of Service attack that comes from multiple devices is called a Distributed Denial of Service (DDoS) attack. This is the mechanism many hackers use to prevent online systems from functioning properly.

Services Minister Stuart Robert blamed the recent MyGov crash on a targeted Distributed Denial of Service (DDoS) attack, rather than the website's inability to handle the amount of people seeking access. He later redacted his claim, saying: "DDoS alarms showed no evidence of a specific attack".

Read more: Hacked by your fridge: the Internet of Things could spark a new wave of cyber attacks

Not too late

It was obvious well before Sunday that additional social welfare would be required when COVID-19 left thousands unemployed. The government has no excuse for not organising additional computing resources.

Services Australia, co-owner of the MyGov and Centerlink systems, should have increased the number of allowable users on the website at one time, before this need became a national issue.

Until the government adopts elastic computing strategies, essential online services will keep failing under pressure. If events from earlier this week are any indication, it's safe to say this transition would be better late than never.

[Cybersecurity](#)[Centrelink](#)[Hospitality](#)[Social services](#)[Coronavirus](#)[DDoS](#)[Distributed Denial of Service \(DDoS\) Attack](#)[Coronavirus 2020](#)