404: Infraestruturas Críticas Not Found

digitalinside.pt/404-infraestruturas-criticas-not-found

Bruno Castro

O apagão que afetou simultaneamente várias regiões de Portugal e Espanha evidencia, de forma particularmente preocupante, a enorme vulnerabilidade das infraestruturas críticas numa sociedade cada vez mais interdependente e digitalizada. Num momento tínhamos luz, internet e relativa normalidade; no momento seguinte, estávamos a olhar para o teto como quem espera que o router volte a piscar. Para alguns, talvez não tenha sido propriamente uma surpresa ter acontecido, mas sim uma questão de, quando aconteceria. Surpreendente é o facto de continuarmos a tratar infraestruturas críticas como se fossem gadgets descartáveis – quando, na prática, sustentam tudo o que nos permite funcionar enquanto sociedade.

Num mundo onde quase tudo é *always on*, um apagão não é apenas uma falha de energia – é um *timeout* existencial. Desde semáforos a servidores DNS, desde hospitais a transportes, toda a arquitetura da vida moderna é construída sobre um pressuposto: continuidade. Mas como qualquer engenheiro também sabe, a falha é inevitável. A verdadeira questão é: o que acontece quando ela chega?

Este apagão expôs algo que os especialistas em cibersegurança, redes e engenharia de sistemas têm vindo a alertar há anos: a nossa alta dependência de infraestruturas digitalizadas e interligadas é tão profunda quanto negligenciada. Os sistemas que geram energia, comunicações e transportes estão muitas vezes ligados em redes, com segurança por vezes ad hoc, e interdependências pouco mapeadas. Basta um *bug*, um *glitch*, ou – pior ainda – um *payload* malicioso bem orquestrado, e o efeito dominó começa.

Efeito esse, que vem acompanhado de desinformação e, assim que a luz vai abaixo, acende-se o pânico digital. Várias narrativas surgem, várias explicações contraditórias que criam o sentimento de que é cada vez mais difícil obter a verdade. Quando os sistemas de confiança falham, o resultado é o caos. A seu tempo as origens serão conhecidas, e até lá, especulações não passam disso mesmo. O importante nesta fase é perceber como prevenir situações semelhantes no futuro. É preciso repensar os nossos sistemas críticos, porque efetivamente o são. Isso significa redundância real, testes de resiliência, simulações regulares e monitorização contínua. Significa também tratar a cibersegurança como parte do design, e não como um *patch* tardio.

Adicionalmente, é urgente melhorar a comunicação em tempos de crise. Não basta ter backups dos dados, precisamos de backups da confiança. Planos de contingência devem incluir mensagens claras, canais alternativos de comunicação e combate ativo à desinformação. O apagão tornou clara a importância da comunicação digital e como a ausência da mesma têm a capacidade de alimentar o caos.

Este apagão foi mais uma manifestação de uma realidade para a qual ainda não estamos prontos e um verdadeiro apelo à ação, antes que a próxima falha nos encontre novamente desprevenidos, e de novo, a luz se apague. Um futuro em que grupos organizados – muitas vezes patrocinados por Estados – conseguem atacar e fazer parar um Estado inimigo é cada vez mais uma realidade possível. Sejam avarias ou ataques premeditados, as infraestruturas merecem particular atenção e o reforço da sua proteção. Resta saber se vamos, de facto, aprender com o *stack trace*, ou se continuaremos apenas a reiniciar o sistema, à espera que magicamente nunca volte a falhar.