Report: Without safeguards, Internet and IoT may create surveillance states in near future

Bradley Barth | SC Media| September 2017

A catastrophic worldwide cyberattack, the emergence of an IoT-enabled surveillance state, and the weakening of encryption were among the chief security and privacy fears expressed by experts who were polled for a sweeping new report about the internet and its future impact on mankind.

The 2017 Global Internet Report, published by the non-profit Internet Society (ISOC), is the culmination of an 18-month research project aimed at predicting what factors will most influence the internet's evolution in the next five-to-seven years, and the impact of such changes. To get a consensus view of the internet's prospects, the organization surveyed 3,000 members, professionals and partners in 160 countries.

According to the study, stakeholders worldwide still believe that the internet's benefits will continue to outweigh the risks in the coming years, transforming lives through the efficient delivery of critical services and revolutionizing industries across multiple sectors. But they also sense that the threat is growing, especially as businesses create new attack vectors by relying on a growing number of interconnected data sources.

"Cybersecurity will be the most pressing challenge of the next decade," the report states. "Responses to date have been thoroughly insufficient and the costs are escalating." And based on recent precedent, "…it is not far-fetched to imagine a digital pandemic with attacks crippling entire economies."

The ISOC also expects to see more destructive acts of cyber war, coupled with online disinformation campaigns in an effort to destabilize countries and their economies. However, the organization believes these acts will be perpetrated by not only nation-states, but also "their surrogates, and by independent political movements and private actors."

Ultimately, the growth of the internet could largely depend on how well the security community at large responds to attacks, the report cautions. With the stakes so high, some nations may feel compelled to scale back online freedoms and restrict global connectivity in the name of national security,

resulting in the creation of “walled gardens,” the balkanization of the internet, and the weakening or banishment of encryption technologies. Indeed, ISOC’s survey-takers generally said they believe future government regulations will be more intrusive and restrictive than they are today.

To prevent such a scenario, the report calls for “new accountability, incentive and liability models” to “increase cybersecurity readiness and reduce vulnerabilities but also to ensure end-user security.” The ISOC is also pushing for worldwide, multi-stakeholder collaboration to address these threats, as opposed to fragmented, unilateral efforts.

“I think there are some major architectural changes which need to take place in the internet, and I’d like to see more effort put forward [toward] new innovative architectural changes,” said Leonard Kleinrock, a renowned computer scientist, considered among the fathers of the internet, in an ISOC webcast panel discussion on Monday.

But even such architectural changes won’t necessarily secure the “edge” of the internet, where IOT devices reside. This unprotected edge, where you’ll find devices “put together by a small company, thrown on your wall with a camera, with a microphone, with access to the internet in a typically unprotected, insecure fashion – that’s where the penetrations will take place,” Kleinrock added.

Perhaps it’s no surprise then that the ISOC devoted a large section of its report to IoT devices, noting that as we rapidly approach a connected world, devices will generate and collect vast amounts of personal user data that nations could potentially leverage to create a surveillance state.

In addition to seeing even more attacks from threats modeled after the Mirai IoT botnet, “We may see increased mass surveillance, the further erosion of privacy, and a growing dependence on data collection, analytics, and curation,” the report states. “The implications for privacy are profound. Without essential safeguards, greater amounts of data will be collected and used without the user’s knowledge or control.”

ISOC has recommended pursuing a collaborative and proactive effort among stakeholders to instill effective IoT safeguards. For instance, device manufacturers and service providers should be taking steps to bake privacy and security into the actual design process, the report suggests, while the insurance industry could do its part by requiring IoT devices to have security certifications before owners of these products can be insured.