Vom humanoiden Roboter bis zum Fake President

08.10.17 | Berlin | Haus der Wirtschaft

Vom humanoiden Roboter bis zum Fake President

IT-Experten informieren über sicherheitsrelevante Themenfelder in Fertigung und Büro

Die Zahl der Angriffe im World Wide Web nimmt rapide zu. „WannaCry“ und „notPetya“ sind nur zwei der jüngsten Attacken, die vielen Unternehmen weltweit ordentlich zu schaffen machten. Allein „WannaCry“ infizierte in über 150 Ländern Windows-Rechner und sorgte für massive Beeinträchtigungen. Das Hauptproblem: Viele Unternehmen unterschätzen das Risiko weiterhin und tun zu wenig für die digitale Sicherheit vom und am Arbeitsplatz.

Um das Bewusstsein hierfür zu schärfen und Lösungsansätze aufzuzeigen, luden der Verein Sichere Identität Berlin-Brandenburg e. V. und die UVB am 5. Oktober zum zweiten World Café „Digitale Sicherheit“ ein. Anlass war die Aktionswoche „Cybersicherheit am Arbeitsplatz“ – im Rahmen des European Cybersecurity Month. An fünf Thementischen präsentierten Experten Lösungen für die digitale Sicherheit in Fertigung und Büro – im Fokus sichere Identitäten.

„Das Thema Cybersicherheit betrifft alle Bereiche“, leitete Sven Weickert, Geschäftsführer der Unternehmensverbände Berlin-Brandenburg die Runde ein. „Von der E-Mail-Sicherheit über Roboter-Sicherheit bis hin zu IoT im Werk ist die Bandbreite groß. Und alle Systeme müssen

gleichermaßen gegen Cyberattacken geschützt sein.“ „Doch woher weiß ich, wie sicher ich bin? Und wie kann ich echte von gefälschten digitalen Dokumenten unterscheiden?“, griff Anne-Sophie Braun, Geschäftsführerin des Vereins Sichere Identität Berlin-Brandenburg das Thema auf. „Diese Fragen werden uns heute an unseren Thementischen beschäftigen“.

Tisch 1: Die Prüfung von IT-Sicherheit

Für Unternehmen heißt die Beschäftigung mit IT-Sicherheit auch immer das Abwägen von Kosten und Nutzen. Denn Investitionen können nicht gleich 1:1 in einen monetären Mehrwert umgerechnet werden. Ihr Nutzen zeigt sich oft erst, wenn Cyberkriminelle tätig werden. Entsprechend investieren viele Unternehmen nur wellenförmig in ihre IT-Sicherheit. Immer wenn ein Angriff für Unsicherheit sorgt, oder schlimmstenfalls der Schaden schon entstanden ist, wird investiert. Jedoch ist ein wirklich guter Sicherheitsstandard nur durch kontinuierliche Investitionen zu erreichen.

Dafür gilt es, das Thema Cybersicherheit fest in der Unternehmensstrategie zu verankern. Jedes Unternehmen sollte all seine Datenbestände dahingehend überprüfen, welche Daten wirklich schützenswert sind und welche eben nicht. Anschließend gilt es, zusammen mit IT-Experten Sicherheitsmaßnahmen für die schützenswerten Daten umzusetzen.

Eine kontinuierliche Beschäftigung mit der eigenen IT-Sicherheit reduziert schließlich auch die Angst vor dem Einsatz digitaler Techniken und bringt im digitalen Wandel voran. Dabei ist immer abzuwägen, wie hoch das Sicherheitsrisiko ist, wie gut Schutzmaßnahmen greifen und wie stark ein Verzicht auf den Einsatz digitaler Technik die Arbeitsfähigkeit einschränken würde.

Tisch 2: Cyber-Dokumentenfälschung nimmt zu

Auch im Fälschen von Cyber-Dokumenten haben Kriminelle ein lukratives Feld entdeckt. Hier helfen digitale Werkzeuge, sich vor Missbrauch zu schützen. Neben dem Public-Key-Verfahren für elektronische Unterschriften, kann beispielsweise das elektronische Siegel für Sicherheit sorgen. Als digitaler Unternehmensstempel für juristische Personen schützt es digitale Dokumente vor Manipulationen.

Tisch 3: Social engineering

Im Durchschnitt haben wir 25 verschiedene Identitäten im Netz. Und durch den digitalen Wandel werden es stetig mehr. Jede Kamera, jeder Sensor hat seine eigene Identität. Entsprechend groß ist das kriminelle Potenzial. Mit dieser Thematik beschäftigt sich das Fachgebiet „Social engineering“.

Der „Fake President“ ist nur eines der Fallbeispiele, wie Hacker mit einer falschen Identität Unternehmen um Millionenbeträge berauben können. Dabei erhält ein Mitarbeiter, vorzugsweise aus der Buchhaltung, eine E-Mail, die augenscheinlich vom obersten Chef kommt. Dieser bittet den Mitarbeiter darum, ein wichtiges Geschäft vertrauensvoll vorzubereiten und einen bestimmten Geldbetrag zu transferieren. Gerade in großen Unternehmen mit vielen Hierarchieebenen fällt der Betrug meist erst auf, wenn es schon zu spät ist.

Abwehr gelingt nur durch transparente Kommunikation und klare Absprachen über alle Ebenen hinweg. Doch insbesondere das Schaffen der nötigen Transparenz in der obersten Führungsebene fällt vielen Unternehmen immer noch schwer.

Tisch 4: Roboter in der Fertigung

Humanoide Roboter als Zeitarbeiter in der Fertigung? Was nach Zukunftsmusik klingt, setzt die Berliner pi4_robotics bereits um. Die Roboter übernehmen einfach zu erlernende Tätigkeiten in der Wertschöpfungskette und verschaffen den Mitarbeitern so Zeit für wertvollere Aufgaben. Auch das wird künftig mehr und mehr Thema werden. Zwar sind Mensch-Maschine-Kollaborationen in Form der direkten Zusammenarbeit von Mitarbeitern und Robotern heute noch nicht möglich, jedoch übernehmen Roboter bereits zahlreiche automatisierte Arbeiten in den Werkshallen. Und dabei werden sie mehr und mehr vernetzt – ein Thema, das auch die IT-Sicherheit immer stärker beschäftigen wird. Denn was passiert, wenn ich nicht möchte, dass mein Zeitarbeiter-Roboter die in meinem Betrieb erlernten Fähigkeiten in die Cloud einspeist und so mitnimmt?

Tisch 5: Das industrielle Internet der Dinge in der Fertigung

Wie Fog- und Edge-Computing Daten und Werker schützen können, war Schwerpunkt des fünften Thementisches beim World Café. In der Edge-Technologie sieht Experte Thomas Grütter vom Fraunhofer Institut die Zukunft. Denn immer mehr digital vernetzte Geräte produzieren immer mehr digitale Daten, die in der Cloud kaum noch verarbeitet werden können. Um den Daten-Traffic im Backend entsprechend zu verringern, werden die Daten deshalb mittels Edge-Computing direkt an den Mobilfunkstandorten verarbeitet. Das sorgt für Schnelligkeit, aber auch neue Sicherheitsanforderungen. Denn Datenhoheit und Datensicherheit nehmen ab, je weiter man sich Richtung Edge bewegt.

So gab jeder Thementisch des World Cafés einen kurzen Einblick in die sicherheitsrelevanten Fragestellungen, die sich ein modernes Unternehmen heute stellen muss. Wichtig ist, dass Unternehmen beginnen, sich intensiv mit dem Thema Cybersicherheit auseinanderzusetzen und Lösungen zu suchen. Eine 100%ige Sicherheit gibt es nach Ansicht der Experten nie, aber eine strategische Verankerung im Unternehmen und kontinuierliche Investitionen in die Datensicherheit, können das Risiko deutlich minimieren. Ein positiver Nebeneffekt: Die Angst vor neuen digitalen Techniken sinkt mit der Sicherheit, die Unternehmen dazugewinnen.

Bild

Sven Weickert, Geschäftsführer der Unternehmensverbände Berlin-Brandenburg © UVB 2017

Bild

Anne-Sophie Braun vom Verein Sichere Identität Berlin-Brandenburg e.V. © UVB 2017

Bild

Prof. Dr. Thomas Thiessen, Mittelstand 4.0 Agentur Kommunikation © UVB 2017

Bild

Fünf Thementische bildeten die inhaltlichen Schwerpunkte des World Cafés. © UVB 2017

Bild

Thementisch 5: Das industrielle Internet der Dinge in der Fertigung – Wie Fog- und Edge-Computing sowohl Daten als auch Werker schützen können. © UVB 2017

Bild

Thementisch 4: Roboter in der Fertigung © UVB 2017

Bild

Thementisch 3: Social engineering: Gefahr von Schaffung neuer Identitäten am Arbeitsplatz © UVB 2017

Bild

Das anschließende Get-together nutzten Experten und Teilnehmer, um sich zu den Fragen rund um die Cybersicherheit auszutauschen. © UVB 2017

- Auf Xing teilen
- Auf Facebook teilen
- Auf X teilen
- Auf LinkedIn teilen

- Drucken
- Als PDF speichern

Dokumentation zum 1. World Café

Dokumentation zur Dialogveranstaltung "Sichere Identität" vom 11.05.2017

Download (PDF 1,8 MB)

Veranstalter

SICHERE IDENTITÄT
BERLIN BRANDENBURG

UVB
Unternehmensverbände
Berlin-Brandenburg

In Kooperation mit:

Mittelstand 4.0
Agentur
Kommunikation

Mittelstand-
Digital

Ihre Ansprechpartner

Geschäftsführerin
Anne-Sophie Braun
Sichere Identität Berlin-Brandenburg e.V.

E-Mail: info@sichere-identitaet-bb.de
Telefon: +49 30 2515-077

Stellvertretender Hauptgeschäftsführer

Sven

Weickert

Telefon:
+49 30 31005-141

Telefax:
+49 30 31005-240

E-Mail:
Weickert [at] allgemeiner-verband.de

Download VCF

Arbeitswissenschaft

Uwe

Radloff

Telefon:
+49 30 31005-142

Telefax:
+49 30 31005-154

E-Mail:
Radloff [at] allgemeiner-verband.de

Download VCF